NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

WHAT'S MY LANE? IDENTIFYING THE STATE GOVERNMENT ROLE IN CRITICAL INFRASTRUCTURE PROTECTION

by

Timothy S. Donnelly

March 2012

Thesis Advisor:	Christopher Bellavita
Second Reader:	Nadav Morag

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2012	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE What's My Lane? Identifying the State Government Role in Critical Infrastructure Protection		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Timothy S. Donnelly			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number _____N/A_____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

What constitutes an effective Critical Infrastructure and Key Resources (CIKR) protection program for Massachusetts? This study evaluates existing literature regarding CIKR to extrapolate an infrastructure protection role for Massachusetts. By reviewing historical events and government strategies regarding infrastructure protection, Chapters I and II will provide scope and context for issues surrounding critical infrastructure. Chapter III reviews the roles of the Department of Homeland Security and the Department of Defense, possibly the two most influential organizations tasked to support the federal infrastructure protection initiative.

Chapter IV analyzes the private-sector role in infrastructure protection as articulated in federal strategies, academic research, federally directed studies, and professional journals. The National Infrastructure Protection Plan's framework for managing the risk to CIKR will be used as a guide in Chapter V to evaluate the infrastructure protection strategies of Arizona, Virginia, and Washington.

Finally, Chapter VI recommends that Massachusetts develop a state infrastructure assurance program vice a Critical Infrastructure Protection Program. Concepts such as reframing the critical infrastructure debate, creating infrastructure public/private partnerships and information sharing processes to build trust among the entities invested in ensuring the delivery of infrastructure services are recommended for inclusion in a state infrastructure assurance strategy and subsequent infrastructure assurance program.

14. SUBJECT TERMS Strategic role, critical infrastructure protection, Critical Infrastructure and Key Resources (CIKR), infrastructure public-private partnerships, infrastructure assurance program, infrastructure assurance strategy, risk management, delivery of infrastructure services, critical infrastructure protection, infrastructure resilience, public resilience	**15. NUMBER OF PAGES** 153
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

WHAT'S MY LANE? IDENTIFYING THE STATE GOVERNMENT ROLE IN CRITICAL INFRASTRUCTURE PROTECTION

Timothy S. Donnelly
Sergeant, Massachusetts State Police
Aviation Security, Logan International Airport, Boston, Massachusetts
B.S., University of Lowell, 1984

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
March 2012

Author: Timothy S. Donnelly

Approved by: Christopher Bellavita
Thesis Advisor

Nadav Morag
Second Reader

Daniel Moran
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

What constitutes an effective Critical Infrastructure and Key Resources (CIKR) protection program for Massachusetts? This study evaluates existing literature regarding CIKR to extrapolate an infrastructure protection role for Massachusetts. By reviewing historical events and government strategies regarding infrastructure protection, Chapters I and II will provide scope and context for issues surrounding critical infrastructure. Chapter III reviews the roles of the Department of Homeland Security and the Department of Defense, possibly the two most influential organizations tasked to support the federal infrastructure protection initiative.

Chapter IV analyzes the private-sector role in infrastructure protection as articulated in federal strategies, academic research, federally directed studies, and professional journals. The National Infrastructure Protection Plan's framework for managing the risk to CIKR will be used as a guide in Chapter V to evaluate the infrastructure protection strategies of Arizona, Virginia, and Washington.

Finally, Chapter VI recommends that Massachusetts develop a state infrastructure assurance program vice a Critical Infrastructure Protection Program. Concepts such as reframing the critical infrastructure debate, creating infrastructure public/private partnerships and information sharing processes to build trust among the entities invested in ensuring the delivery of infrastructure services are recommended for inclusion in a state infrastructure assurance strategy and subsequent infrastructure assurance program.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ASIS	American Society for Industrial Security
BZPP	Buffer Zone Protection Program
C/ACAMS	Constellation/Automated Critical Asset Management System
CBAT	Computer Based Assessment Tool
CIKR	Critical Infrastructure and Key Resource
CAPTAP	CIKR Asset Protection Technical Assistance Program
CIP	Critical Infrastructure Protection
COOP	Continuity of operations
CPIMD	Contingency Planning and Incident Management Division
CRS	Congressional Research Service
DCI	Defense Critical Infrastructure
DCIP	Defense Critical Infrastructure Program
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DIS	Defense Infrastructure Sector
DISLA	Defense Infrastructure Sector Lead Agent
DoD	Department of Defense
EO	Executive Order
ESF	Emergency Support Function
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
FLETC	Federal Law Enforcement Training Center
FOIA	Freedom of Information Act

FSLC	Federal Senior Leadership Council
GAO	Government Accountability Office
GCC	Government Coordinating Councils
HD&ASA	Homeland Defense & America's Security Affairs
HITRAC	Homeland Infrastructure Threat and Analysis Center
HSPD	Homeland Security Presidential Directive
IA	Infrastructure Assurance
IASD	Infrastructure Analysis and Strategy Division
IDW	Infrastructure Data Warehouse
IICD	Infrastructure Information Collection Division
IP	Infrastructure Protection
IPSC	Infrastructure Protection Sub Committee
ISCD	Infrastructure Security Compliance Division
MIST	Multimodal Information Sharing Team
NIPP	National Infrastructure Protection Plan
PCII	Protected Critical Infrastructure Information
PDD	Presidential Decision Directive
POD	Partnership and Outreach Division
PSA	Protective Security Advisor
PSCD	Protective Security Coordination Division
SCC	Sector Coordinating Councils
SLTTGCC	State, Local, Tribal and Territorial Government Coordinating Council
SSA EMO	Sector Specific Agency Executive Management Office
SSP	Sector Specific Plan

SSSC	State Sector-Specific Councils
TSA	Transportation Security Administration

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

This thesis serves to identify strategic roles that the state of Massachusetts should fulfill to effectively secure the delivery of infrastructure services within its jurisdiction. Review of federal Critical Infrastructure and Key Resource (CIKR) plans and strategies, other states' CIKR protection plans or strategies, academic research and other writings on the topic provide sufficient rationale to propose a state government role in Critical Infrastructure Protection (CIP). The conclusions garnered from this research provide the framework for an effective infrastructure assurance program and a CIKR assurance strategy for the state of Massachusetts. A successful infrastructure assurance program would require the following steps to be implemented:

- Reframe the infrastructure protection narrative;
- Develop resilience in infrastructure and the public;
- Write a state CIKR protection strategy and develop an effective state CIP program;
- Select an experienced, knowledgeable and influential individual to lead the CIP effort;
- Educate CIP practitioners, politicians and the public;
- Develop appropriate public/private partnerships and sector-specific councils; and
- Create trust through transparent information sharing.

A. REFRAME THE NARRATIVE

1. Infrastructure Assurance

It is necessary to reframe the CIKR protection narrative in order to effectively manage the viability of infrastructure in this country. The nation's current infrastructure narrative became focused on security of infrastructure rather than ensuring that

infrastructure remains viable to deliver service. This narrative has been further distorted since 9/11, when the definition of “critical infrastructure” expanded to our current list of 18 CIKR sectors.

To better focus the infrastructure assurance effort and rein in the critical infrastructure mission creep, it is necessary to better define what infrastructure is critical as opposed to what is normal. The overarching infrastructure narrative should be oriented toward the assured delivery of services, rather than simply protecting CIKR. The goal of an infrastructure assurance strategy would be to provide targeted support to the infrastructure sectors, both from government and the private sector, so that quality services are delivered consistently and—if there is a disruption—that “critical” service is returned as quickly as practical. Services deemed to be critical would receive priority support toward the assured delivery of service based upon a predefined ranking structure or process.

2. The New Critical

Within the state of Massachusetts infrastructure effort there should be two distinct categories of infrastructure: one “critical,” the other “normal.” Infrastructure deemed “critical” would qualify for regular maintenance support and prioritized protection effort, while the infrastructure deemed “normal” would qualify for the investment of resources oriented toward regular maintenance. During recovery operations in the aftermath of a significant manmade or natural disaster, infrastructure providing critical service would receive priority efforts to restore its associated service. Assurance of service requires the investment of capital and other resources in both types of infrastructure. Both types of infrastructure should be designed and operated with resilience in mind.

3. Understanding the Threat

The infrastructure protection debate needs to be reframed in the context of better understanding the threats from which we are trying to secure infrastructure.

An accurate threat picture is necessary to conduct worthwhile risk assessments that drive infrastructure assurance decisions. Excluding the attacks of 9/11, the direct result of the

majority of terror attacks does not achieve the level of strategic effect that warrants the expenditure of resources applied by the United States across the many infrastructure sectors. Experienced state CIP practitioners need to engage the Department of Homeland Security (DHS) and challenge the homeland security paradigm, specifically in the area of risk assessment and threat assessment. State CIP practitioners should be informed and experienced in the spectrum of threats enough to challenge threat and risk assessments that don't comport with their understanding of the regional threat. The aggregate of localized threat should be contained in an annual risk assessment that provides a context to understand how a threat may make CIKR in our region vulnerable.

B. DEVELOP RESILIENCE IN INFRASTRUCTURE AND THE PUBLIC

A state CIP program should be involved in identifying critical infrastructure in its jurisdiction worthy of investment in redundant capacity and helping to guide the development and implementation of effective management processes to avoid or respond to infrastructure disruptions. The federal solution of creating resilience to mitigate the effects of either man-made or natural threats is encouraged through the 2009 NIPP. Resilience is the best alternative to mitigate the spectrum of predictable and unpredictable threats facing infrastructure. Infrastructure resilience to threats of man or nature can be achieved by creating redundant capacity through construction of back-up facilities to replace damaged buildings or through effective management processes and procedures that avoid disasters or efficiently recover from them. Building redundancy through back-up buildings or through engineering more robust systems can be prohibitively expensive.

The state infrastructure assurance program can assist the federal government, the state government, the private sector, and the public to develop the appropriate resiliency. The state infrastructure assurance program should also help emergency managers and private sector asset owners to coordinate and exercise effective response capability within their jurisdiction. State government has a role to enhance the resilience of its population by building the resolve and capacity of the population to support itself for short periods during an emergency.

C. DEVELOP A STATE INFRASTRUCTURE ASSURANCE STRATEGY AND AN EFFECTIVE INFRASTRUCTURE ASSURANCE PROGRAM

1. Infrastructure Strategy

At this time, Massachusetts is without a state CIKR protection strategy. The state must develop a strategy oriented toward a new concept of overall infrastructure assurance to include a more focused component that addresses CIKR protection of assets warranting a greater level of support. State government roles must be articulated in a comprehensive infrastructure protection strategy that acknowledges the various efforts of public- and private-sector partners and synchronizes those efforts toward insuring the delivery of infrastructure services in the jurisdiction. To synergize with the federal CIKR effort, Massachusetts should develop a strategy that utilizes the NIPP risk management framework as a guideline, similar to the strategies of the commonwealth of Virginia and the state of Washington. With respect to synchronizing partnerships, there are elements of the Virginia and Washington plans that bear inclusion in the Massachusetts strategy. In addition to incorporating some of the highlights from the Virginia and Washington plans, Massachusetts should develop more detailed goals, define who is responsible to accomplish those goals, and legislate funding to sustain the initiative.

2. State Infrastructure Program

The state of Massachusetts must create a broad infrastructure assurance (IA) program that focuses on assuring infrastructure's consistent delivery of service. The program must be mandated in legislation. The infrastructure assurance program would maintain an inventory of the "normal" infrastructure, as well as the "critical" infrastructure. Within the state infrastructure assurance program, there must be a subgroup that focuses exclusively on the "critical" infrastructure in the state and on steps to ensure that critical infrastructure is effectively secured from threats.

The infrastructure assurance program should be made up of members representing multiple disciplines and multiple agencies from state and federal government, and it should include representatives from the private sector and academia. A broad coalition of

team members will ensure a breadth of experience and professionalism and will act to spread the burden of inventorying and assessing infrastructure assets within the state across all interested entities. Considering the task of the Department of Defense (DoD) to secure the Defense Industrial Base (DIB) and a state's obligation to assist the DoD in that regard, the state's national guard should have representatives on the teams.

D. STATE INFRASTRUCTURE PROGRAM LEADER

Much as an orchestra is led by a conductor, the IA program will require a leader to arrange the appropriate scores or plans, cultivate members' skills, and blend the skills to achieve an effective program. The stable of IA program members can be likened to the members of an orchestra with honed skills who require organization to produce a symphony. The current CIP program of the state of Massachusetts should become the infrastructure assurance program within the office of the Secretary of Public Safety, directed by the Under Secretary for Homeland Security. The under secretary is better positioned to engender the cooperation and goodwill of the many entities with a vested interest in CIP. Whoever leads this program should posses the organizational skills of a maestro and demonstrate the ability to orchestrate a multiagency, multidisciplined effort.

E. EDUCATE CIP PRACTITIONERS AND POLITICIANS

The current CIP practitioner's challenge to secure CIKR is compounded by a limited understanding of the composition of modern infrastructure, the interconnections and dependencies between assets within an infrastructure sector and across sectors, and the nature and degree of threats that make CIKR vulnerable, and from a lack of credible data that validates which protection actions are the most effective and resource-efficient to ensure the delivery of service. An initial objective of the state strategy is to promote a mechanism to develop the appropriate knowledge and skills in the infrastructure assurance program members and a corporate understanding of what is critical in the infrastructure sectors represented in Massachusetts. That corporate knowledge can be developed, consolidated, and shared in local colleges or shared in public-private partnerships.

The education and research efforts undertaken by George Mason University in partnership with government and private industry should be a model for Massachusetts to mirror in one of its local universities. State infrastructure assurance practitioners can hone their skills in such an academic relationship while academics would benefit from their interaction with private-sector and public-sector CIP practitioners who may share ideas about the direction that research should take. Ultimately, public- and private-sector CIP practitioners' participation in CIP educational opportunities offered at universities and colleges will foster the development of future "maestros" and "virtuosos" of homeland security.

The director of the state IA program should engage local and state politicians to encourage their support of the goal of statewide infrastructure assurance. Political support can be made more effective by educating politicians about infrastructure assurance. Political support and understanding of the infrastructure assurance goal may help to eliminate the manipulation of public fears in order to gain consensus toward funding security programs that are not necessary. Politicians may best serve the infrastructure assurance effort by endorsing more research in the areas of infrastructure interdependencies, network vulnerabilities, and metrics to measure the effectiveness of infrastructure protection efforts; by promoting education and training for CIP practitioners; and by promoting public-private partnerships.

F. DEVELOP PUBLIC-PRIVATE PARTNERSHIPS AND SECTOR-SPECIFIC COUNCILS

The state of Massachusetts should develop public-private partnerships to facilitate its infrastructure assurance initiative. The infrastructure assurance partnership should be organized along the lines of a "megacommunity" partnership. The megacommunity partnership concept primarily consists of three sectors: government, civil society, and business. The objective of Massachusetts government should be to exploit the dynamic tension between the three primary sectors mentioned above to unify infrastructure assurance partnerships toward achieving a common interest of infrastructure assurance.

The state infrastructure assurance program must encourage the partnerships but not feel compelled to lead the partnership effort. The need is not for a single leader for these partnerships but rather a common understanding of the objective of infrastructure assurance and a corporate desire to achieve it. The partnerships should be encouraged to self-govern their actions and work cohesively toward achieving the state's strategic objectives.

In addition to developing partnerships, the state of Massachusetts would be well served to develop state sector-specific councils (SSSC). The directors of the SSSCs would report to the director of the state infrastructure assurance program. One significant benefit of the SSSC is that the state is able to delegate responsibility for providing oversight of an entire infrastructure sector to an SSSC working on behalf of the state infrastructure assurance program. The director of the SSSC would function like the section leader of an orchestra, by organizing the associated infrastructure sector to perform at the direction of the state infrastructure protection maestro.

G. CREATE TRUST THROUGH INFORMATION SHARING

Accurate intelligence at the strategic, operational, and tactical level is necessary for infrastructure protection practitioners to develop appropriate security programs to mitigate potential threats. Information sharing issues in the homeland security environment are generally oriented around concerns about the federal government's sharing intelligence and threat information with state government, with the private sector or across any combination of those supposed partners**.** The fact that many private-sector asset owners do not get actionable intelligence leads them to conclude that government is unwilling to share relevant intelligence with them, rather than understanding that they are not getting the intelligence they expect because there that type of intelligence is not available. State government needs to develop trusting relationships, in which its private-sector partners accept that, when the state has actionable intelligence of a direct and predictable threat to their industry, they will be apprised of the information.

In addition to intelligence information, more generalized information sharing is a necessary practice to achieve infrastructure protection and the assured delivery of service. For example, a public-private infrastructure assurance partnership should regularly share ideas on how to most effectively work together to achieve common understanding.

ACKNOWLEDGMENTS

I thought I would avoid writing an involved acknowledgement for my thesis. I was wrong. Completing this thesis became such a journey that I considered changing my name to Odysseus. However, lacking a Greek heritage and god-like qualities, I elected not to. I am compelled, though, to recognize those who endured my journey. Sincere thanks and love to my wife, Jane, whose support, as I know best, was unwavering and whose patience could cause Job to envy. Love and thanks as well to my daughter, Laura, whose commitment to life is inspiring. To those in my family and my professional communities who gave support through their patience, thank you. To my “high functioning” friend Jose, thanks for the numerous nudges, pushes, and the willingness to read this. Dr. Morag, and all of CHDS (even for those who lost the bet), thank you for your commitment to all of us. I owe an enduring debt of gratitude to Dr. Bellavita, who is recognized by many in my cohort and other cohorts as well as a national treasure. Through this process I am now certain that you are. For you alone I hope for the return of the Brooklyn Dodgers. And finally to my Mom and my sister Moira, I’m sorry not to have completed this thesis while you were with us. Bless you and please negotiate a space for me. I think I’ll need your help. I doubt I would have finished without all of you. Thank you!

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

There is an extensive array of infrastructure in this country that presents a potential target for terrorists. Identifying the infrastructure, quantifying what is critical, as well as understanding the interdependencies and vulnerabilities of that infrastructure to damage, and then developing effective mechanisms to protect that critical infrastructure and key resources (CIKR) is a daunting task. The federal government has identified the importance of critical infrastructure to the nation's continued welfare and prosperity. It has created a number of strategies and plans to coordinate the protection of the nation's CIKR. The federal government understands that the task of identifying and securing the nation's CIKR is Herculean. It wisely acknowledges that it cannot protect all of the CIKR in the country. The federal solution to the CIKR protection task is to categorize and rank critical infrastructure by its relative importance to the country and to focus federal efforts to assess and develop plans to secure the assets with the highest national importance.

The federal critical infrastructure strategies rely on assistance from state governments to support the federal effort to identify and secure assets that are most critical. The state of Massachusetts accepts responsibility to protect CIKR assets within the state that are designated as critically important by both the federal government and the state. The state of Massachusetts has signed on to a complex responsibility.

There is no critical infrastructure protection (CIP) strategy for Massachusetts to guide the endeavor. Federal critical infrastructure protection strategies do not specify how states will protect the infrastructure in their jurisdiction. The state of Massachusetts lacks formal guidance that establishes a critical infrastructure protection program. The state also lacks formal guidance that identifies a vision, goals, objectives, and delineation of the responsibility for the effort required to identify, assess, and secure critical infrastructure in the state. The problem to be studied in this thesis is how to create a state government critical infrastructure protection program that effectively supports the national and state critical infrastructure protection needs.

B. RESEARCH QUESTION

1. What should the roles and responsibilities of state government be with respect to assessing and protecting critical infrastructure assets in their jurisdiction?
2. What could constitute an effective CIKR protection program for the state of Massachusetts?

C. SIGNIFICANCE OF RESEARCH

A significant amount of literature relative to critical infrastructure protection exists. Some of this literature identifies roles for state government in the country's infrastructure protection mission. Two of the more current federal strategies, the 2009 National Infrastructure Protection Plan and the May 2011, National Security Strategy identify state government as a significant partner in the CIP mission. That literature outlines the general concept of state government's role in critical infrastructure protection. Unfortunately, it appears that the federal strategy is based on broad concepts and does not provide specific guidance that identifies how infrastructure will be protected and by whom. The intent of this research is to cull evidence from critical infrastructure protection literature that identifies the federal government's expectations of a state government with respect to CIP, as well as to review literature capturing published lessons learned in the national CIP effort. Other critical infrastructure protection literature will be synthesized and evaluated to define an appropriate state government role to achieve an effective CIKR protection effort. The ultimate objective of this research is to provide a template that could assist the state of Massachusetts and other state governments to develop an effective CIP program with attainable objectives that also support the federal infrastructure protection objectives.

Throughout this thesis, the analysis is influenced by this author's opinion that in the arena of critical infrastructure protection governments are following the guidance of federal strategy without really understanding how to actually achieve the end states, why they are pursuing these efforts, and whether what they are pursuing will be effective. Dr. Christopher Bellavita articulates that sense well when he writes, "Homeland security's

first decade was characterized by 'ready, fire, aim.' A great deal of work had to be done in a short period of time. Much was accomplished during that decade and it cost a lot of money." He writes further, "No one knows how much of that money went to ineffective activities because the homeland security enterprise spent more effort firing than aiming."[1] My objective is to identify where the CIP effort is well-aimed fire to be continued as "effective fire" and where the efforts that constitute firing without aiming should receive the order to "shift fire" or "cease fire."

For future efforts, this author recommends research into the appropriate level of government intervention required to protect or to regulate the protection of privately owned critical infrastructure assets that support our nation. Theoretically, free-market forces should establish the degree of protection necessary to secure infrastructure sectors that support a capitalist society. Presumably, the private sector understands what is required to secure the infrastructure it operates. To compound this issue, the degree of federal intervention required to secure a sector may vary across the different infrastructure sectors. An extension to this debate is whether the private sector should be allowed to own infrastructure that is critical to the welfare of our nation or whether that infrastructure should be owned by the government. Answering those questions is important and complex. Additionally, it is necessary to establish credible criteria and associated metrics that objectively measure the value of the state's CIKR protection effort. In these times of reduced budget and financial constraints, the protection efforts undertaken must target the CIKR that is most vulnerable to damage and, if damaged, will present the greatest loss to the state and country. That CIKR may be a critical node that links multiple components of a sector together or links multiple interdependent sectors where damage to that node will propagate damage across the sector or sectors. Properly securing that CIKR asset should maximize the protection investment for the entire sector or sectors.

[1] Bellavita, "How Proverbs Damage."

D. LITERATURE REVIEW

The literature review that follows will identify the lack of definitive guidance as to what constitutes an effective CIP role for a state government. Much of the government-generated literature on CIP seems to perpetuate the same general concepts articulated in federal homeland security strategies, but it lacks detail on validated protection roles for state government. State government infrastructure protection strategies seem to parrot the language in federal guidance, seemingly to insure that they are competitive for federal infrastructure protection grant funds by impressing the grant application reviewers with their knowledge of federal CIKR guidance. What the literature review will show is the complexity of the CIKR protection issue, and it suggests that the limited understanding of the issue from the state infrastructure protection practitioner's perspective interferes with developing relevant state CIP strategy. This review will also identify the lack of research to validate the government resources expended on critical infrastructure protection. Based on this information, this thesis will outline the scope of the CIKR protection issue from a state perspective, while identifying what we know, what we do not know, what we think we know, and what we need to know to establish an effective CIKR protection effort.

The critical infrastructure that supports our nation's economy and way of life is vast and complex. Not surprisingly, there is a relatively broad spectrum of literature related to critical infrastructure. However, there are no academic studies that identify what an effective critical infrastructure protection program for a state government should look like. In order to posit a viable role for state government in critical infrastructure protection, this author's review focuses on literature with a nexus to protecting infrastructure. To meet the objectives of this thesis, the literature review investigates the following areas:

- The definition of CIKR based upon the history of modern critical infrastructure;
- Guidance relative to identifying and inventorying infrastructure;

- An assessment of CIKR vulnerability to damage from natural or man-made events;
- The securing of networks that support critical infrastructure; and
- Information sharing with federal and private-sector partners.

Much of the available critical infrastructure protection guidance is found in federal government homeland security strategies, Department of Defense (DoD) directives, Congressional testimony and research, state government homeland security strategies, and academic research, journals, and textbooks. These sources are reviewed in the following sections.

1. Federal Government Homeland Security Guidance

A series of presidential directives—from EO 13010 in 1996 to Presidential Decision Directive 63 (PDD 63) in 1998, signed by President Clinton, to Homeland Security Presidential Directive-7 (HSPD-7), signed by President Bush in 2003—demonstrate the evolution in federal thinking about the CIKR issue. The release of EO 13010 was a benchmark indicator that critical infrastructure protection was on the federal government's radar. EO 13010 created the President's Commission on Critical Infrastructure Protection to study the issue and develop understanding in order to make recommendations for action. Members of the commission were to be nominated by the heads of executive branches of the federal government. The commission came to be known as the Marsh Commission, named for the chairman, General Robert T. Marsh, USAF (Retired). The fact that the commission chairman was a retired military officer may be an indication that President Clinton viewed the CIP challenge as the domain of the Department of Defense. EO 13010 identifies eight sectors of infrastructure that the federal government believed, at that time, to be the important critical infrastructure with "vital" importance to the nation's security.[2] Since that time the number of CIKR sectors has grown to its current list of eighteen sectors, which will be identified later in this thesis.

[2] *Executive Order 13010.*

Federal homeland security strategies demonstrate a similar evolution as well. The series of federal homeland security strategies released in the aftermath of the terrorist attacks of September 11, 2001, affords insight into the government's understanding of the world of infrastructure protection at that time and reflects the nation's focus on the threat to infrastructure from terrorism. *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets*, released in 2003, was an initial attempt to coordinate the disparate infrastructure protection efforts being undertaken across the country. Because there were numerous federal strategies referencing the critical infrastructure protection effort, like the National Strategy for the Protection of Critical Infrastructure and Key Assets, the National Infrastructure Protection Plan (NIPP) was created to be the source document on CIP programs nationwide.[3] The 2006 NIPP and the updated 2009 NIPP represent the more recent history and evolution of critical infrastructure protection. The 2009 NIPP is a comprehensive document that provides solid foundational guidance for any infrastructure program. However, the comprehensiveness of the 2009 NIPP translates into a document that may go unread by many in homeland security due to its length.

The 2009 NIPP expanded upon *The National Strategy for Homeland Security* released in October 2007, which, at the time, provided the overarching federal guidance for protecting the homeland. The 2007 National Strategy specifically addresses critical infrastructure protection and broadly identified objectives, such as deterrence of the terrorist threat, mitigating asset vulnerabilities, and minimizing consequences as means of protecting our nation's infrastructure.[4]

The *National Security Strategy* released in May 2010 provides the latest federal vision for securing our nation. In that strategy, President Obama addresses resilience as the integral element to CIKR assurance achieved through a number of actions to include modernizing and upgrading CIKR.[5] The current National Strategy also identifies improving intelligence capacity and information sharing as important elements to CIKR

---

[3] *National Infrastructure Protection Plan,* 2006.

[4] *National Strategy for Homeland Security*, 2007.

[5] *National Security Strategy*, 2010.

assurance. Like many federal strategies the latest National Security Strategy is full of fine rhetoric and good intentions. Whether as a nation we can claim to have turned those strategic words into action and results remains to be seen.

As alluded to earlier, the Department of Defense (DoD) has had experience with security and protection of infrastructure, including infrastructure throughout our nation. Well before 1996, the DoD had been involved in identifying the vulnerabilities of an adversary's infrastructure to disruption from an attack, and it is involved in securing infrastructure that supports our nation's military operations. As such, there is DoD guidance available that identifies the programs that the military utilizes to secure CIKR. DoD guidance could be replicated by a state government as the basis for that entity's infrastructure protection program.

2. Department of Defense Directives

Under Homeland Security Presidential Directive-7 (HSPD-7), the DoD is assigned as the federal agency responsible for the defense industrial base (DIB).[6] In federal homeland security strategies the DIB is identified as one of the nation's critical infrastructure sectors. In addition to defending the United States, the DoD is responsible for ensuring the security of the DIB. An interesting document pertaining to the military's role in our nation's critical infrastructure protection is Department of Defense Directive (DODD) 3020.40, "Defense Critical Infrastructure Program." The directive establishes that,

> Defense Critical Infrastructure, which includes DOD and non-DOD domestic and foreign infrastructures essential to planning, mobilizing, deploying, executing, and sustaining U.S. military operations on a global basis, shall be available when required. Coordination on remediation and/or mitigation shall be accomplished with other Federal Agencies, State and local governments, the private sector, and equivalent foreign entities, as appropriate.[7]

[6] White House, HSPD-7.

[7] *Department of Defense Directive 3020.40*.

Both HSPD-7 and DODD 3020.40 provide a broad overview relative to DoD's responsibility for the security of the DIB, but they do not provide specific information about how protection of that infrastructure sector will be achieved. Although DoD guidance does not specify the role of state government in protecting DIB infrastructure located within a given state's jurisdiction, a state may wish to replicate the DoD's infrastructure protection efforts. State government must also understand the DoD's reliance upon the states and the private sector to help it secure the DIB. Paul Stockton affirms the DoD's historical relationship with state governments with respect to defense support to civil authorities and suggests that the DoD must strongly rely on state government and the private sector to assist in securing CIKR and to assure the delivery of services to the DIB.[8] Stockton's view highlights the need and the value of a partnership among the DoD, state government, and the private sector.

3. Congressional Research and Testimony

Reports of congressional testimony are a wellspring of information that provides insight to the critical infrastructure protection issue. The testimony of the Central Intelligence Agency Director, John Deutch, highlights the threat to our nation that drove protection-related responses. The results of a congressionally mandated investigation captured in the Downing Report establish for the president and Congress the nature of terrorist threats facing the Department of Defense and identify measures to mitigate those threats.[9] Reports from the Government Accountability Office (GAO) based on congressional hearing testimony given by leaders from the private sector, such as the Critical Infrastructure Protection, DHS Leadership Needed to Enhance Cyber Security, offer specific examples of where infrastructure is vulnerable and offer recommendations to mitigate those vulnerabilities.10 Also, research conducted on behalf of Congress by the Congressional Research Service (CRS) provides great insight into CIKR issues debated before Congress. For example, the 2007 CRS Report for Congress, The Department of

[8] Stockton, "Ten Years After."

[9] "Report to the President and Congress."

[10] GAO, "Testimony before the House Committee."

Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress identifies the importance of accurately assessing risk to CIKR.11 The CRS report also addresses the challenges to the awarding of homeland security grant funds based on risk assessment formulas. With respect to a CIP program, a proper risk management assessment strategy is integral to its success. However, the debate suggests that communities utilized inappropriate risk analysis formulas and inflated their community's risk in order to compete for more federal funds. Accurately calculating risk is necessary for government to effectively target funding where it will best secure the nation's infrastructure and not simply satiate a politician's appetite for "political pork." The challenges surrounding risk analysis will be addressed more thoroughly later in this thesis.

4. State Government Homeland Security Strategies

Many states in the nation have written homeland security strategies for their jurisdiction. Arizona was one of the first states to develop a stand-alone infrastructure protection plan. The states of Washington and Virginia have followed and developed infrastructure protection strategies too. Each of these documents provides insight toward how that state intends to secure its people and commerce. In Chapter V this thesis will review those states' CIP strategies to evaluate areas of consensus and divergence with respect to the roles that a state government undertakes in CIP. Also, an analysis of those state CIP strategies reveals where they are synchronized with the guidance recommended in the NIPP. It is not clear whether the state strategies simply parroted the NIPP's guidance to demonstrate the state's support of the NIPP in an effort to compete for federal grant funds.

Unlike Arizona, Virginia, and Washington, Massachusetts does not have a critical infrastructure strategy. Massachusetts has disseminated the *State Homeland Security Strategy*, September 2007, which very generally acknowledges the need for a critical infrastructure program but provides no more guidance as to how that CIP program will be

11 Masse, O'Neil, and Rollins, "Risk Assessment Methodology."

structured.[12] For that deficiency alone, any of the three state CIP strategies identified above could be used as a benchmark strategy for Massachusetts to emulate. The analysis of those state CIP strategies and the NIPP, in conjunction with information gleaned from academic research, journals, and textbooks, will provide the foundation for the CIP strategic actions to be recommended for Massachusetts later in this thesis.

5. Academic Research, Journals, and Textbooks

There is a significant amount of information regarding critical infrastructure captured in academic journals and textbooks. Filtering the literature that is most relevant to my topic poses a challenge. However, a textbook written by Dr. Ted Lewis elucidates some of the complexity of infrastructure protection and should be an important tool to help identify the role of state or local government in infrastructure protection. Dr. Lewis's work, *Critical Infrastructure Protection in Homeland Security*, explains the early history of critical infrastructure and delves into the complexity of networks and the interdependencies that networks create.[13] Another relevant text providing important and broad insight into the CIP issue is *Seeds of Disaster, Roots of Response.* The writings of many of the contributors to the Marsh Commission, as compiled in this book, are an important reference for anyone involved in critical infrastructure protection or for those studying critical infrastructure. The chapter by Brian Lopez, titled "Critical Infrastructure Protection in the United States Since 1993," provides comprehensive insight into the recent history of critical infrastructure.[14]

Another important academic contributor to CIP research exists at George Mason University (GMU) School of Law, Center for Infrastructure Protection and Homeland Security. The CIP research program is strongly influenced by the findings of the Marsh Commission. The GMU research program was developed with Congressional funding, the results of which have produced numerous research papers making significant contributions to the field of CIP. One such study referenced later in this thesis is *Critical*

---

[12] *Commonwealth of Massachusetts State Homeland Security Strategy*.

[13] Lewis, *Critical Infrastructure Protection.*

[14] Lopez, "Critical Infrastructure Protection."

Path: A Brief History of Critical Infrastructure Protection in the United States.[15] This work provides a more extended history of critical infrastructure than will be addressed in this thesis. The GMU CIKR research and commensurate writings should be considered a great resource for professional CIP practitioners.

The history of critical infrastructure just begins to demonstrate the complexity of the CIKR protection challenge. The complex challenge may further be evidenced in areas such as CIKR risk analysis, the fact that CIKR supports communities across the nation and across jurisdictional boundaries, and the apparent depth of competing economic interests across government jurisdictions and private industry with respect to CIP. This complex challenge calls for the development of strategies to manage the problem. There is ample textbook material relative to developing strategy and whether strategy has value and provides a means to an end. John Bryson provides insightful suggestions to guide government and nonprofit strategy sessions in his book *Strategic Planning for Public and Nonprofit Organizations*.[16] Also, the value of a strategic initiative is captured in the book *Megacommunities.* The concept of "megacommunities" was developed by consultants from Booz Allen Hamilton to describe multifunctional partnerships leveraging their cumulative knowledge to solve complex problems.[17] The megacommunity concept will strongly influence the conclusion of this thesis.

6. Summary of Literature Review

The above-mentioned literature reflects what the government and the CIP practitioner knows, thinks they know, and through inference what they need to know about a state government's role in CIKR protection. Throughout the federal government guidance, broad statements, and platitudes are abundant concerning the role of government in CIP. The guidance lacks metrics that demonstrate that the recommended solutions produce an effective and necessary level of protection. The DoD literature represents the military's efforts in CIP, which can enlighten a state government CIP

[15] Brown, *Critical Path*.

[16] Bryson, Strategic Planning.

[17] Gerencser et al., *Megacommunities*.

practitioner but lacks specific, validated recommendations that will achieve a measured degree of CIKR protection. Congressional testimony and research are also deficient in identifying specific roles that state government can undertake to achieve measurable protection results. The state government homeland security strategies lack specific solutions and guidance that will establish an effective CIP program based on measured success. The academic research and studies conducted on the CIP issues begin to establish what an effective CIP program might look like, but they still lack validation. This thesis will evaluate what is known, challenge what is believed to be known, and suggest that the current knowledge is lacking in defining specific actions that are proven to have value, with demonstrable CIKR protection results. The thesis will make the case that in-depth research is needed to establish effective actions for incorporation into a state CIP strategy.

E. METHOD

In order to more fully capture the state of knowledge relative to state government's role in CIKR protection, a more thorough and systematic literature analysis will be conducted to qualitatively identify what critical infrastructure protection is, what roles a state government plays in critical infrastructure protection, what specific actions posture a state to achieve effective critical infrastructure protection, and what are best practices in the field of critical infrastructure protection. Also, a qualitative analysis of relevant CIKR strategies will be conducted to identify whether there are established metrics that validate or disconfirm actions undertaken by state government to provide an effective and appropriate protection posture. The structured analysis of the literature should establish what we know, what we do not know, and what we need to know to ensure that a state government CIKR protection effort provides an effective protection posture.

The literature selection criteria will initially target literature that defines critical infrastructure and the federal government's general role in CIP. The selection criteria will be further guided by the six broad categories of state government CIKR protection actions recommended by the federal government in its 2009 NIPP. The six categories of

action for federal and state governments as described in the NIPP risk management framework are to: "set goals and objectives; identify assets, systems, and networks; assess risks; prioritize CIKR across sectors; implement protective programs and resiliency strategies; and measure the effectiveness of risk-mitigation efforts."[18] Literature that addresses state government's role in achieving each of those six NIPP objectives will be qualitatively assessed to determine whether an effective means of achieving those six objectives exists. A qualitative assessment should also determine what we do not know and what we need to know in the field of infrastructure protection.

[18] *National Infrastructure Protection Plan*, 2009, 163.

THIS PAGE INTENTIONALLY LEFT BLANK

II. WHAT WE KNOW: AN HISTORICAL CONTEXT FOR INFRASTRUCTURE CRITICALITY

An important aspect of CIKR protection is that the CIP practitioner knosw what makes infrastructure critical. This chapter will review four historical events that provide context as to how infrastructure becomes critical and insight as to when infrastructure is critical. As suggested in an edition of the Heritage Foundation's *Backgrounder*, titled *How to Fix Critical Infrastructure Protection Plans: A Guide for Congress*, the use of "critical" as an infrastructure qualifier has undermined the nation's efforts to protect infrastructure that is truly critical.[19] These historical cases will begin to focus the analysis of infrastructure criticality and expose the undercurrent driving CIKR protection concerns.

A. CRITICALITY OF INFRASTRUCTURE DEFINED BY EXAMPLE

Defining the term "critical infrastructure" is necessary to establish the foundation for understanding the issue of critical infrastructure protection. Unfortunately there is no single definition for "critical infrastructure" that clearly frames the boundaries of what constitutes critical infrastructure. Absent a single definition of critical infrastructure, a general understanding of the history of critical infrastructure in this country may help one comprehend when infrastructure becomes critical and establish a framework to better comprehend the Gordian knot facing jurisdictions responsible for protecting CIKR. A review of four incidents since 1962, involving elements of infrastructure, will demonstrate how infrastructure is critical. The historical review will also highlight the ever-changing nature of infrastructure and the increasing complexity of infrastructure sectors over a relatively brief period of time. The reality of the ever-growing complexity of infrastructure and the potential threats to it will demonstrate the need for the state CIP practitioner to be invested in remaining well read and current in the dynamic world of infrastructure protection.

[19] McNeil and Weitz, "How to Fix."

1. The Telephone System

According to Dr. Ted Lewis, the specific phrase "critical infrastructure protection" was not used in print until 1997. However, as Dr. Lewis explains in his book *Critical Infrastructure Protection in Homeland Security*, the evolution of infrastructure protection began with the need to ensure a more secure telephone system after phone communications between President Kennedy and Premier Khrushchev were disrupted 30 years earlier during the Cuban Missile Crisis.[20] The telephone system during that crisis reportedly did not provide reliable service during the tense negotiations between the two world leaders or between Kennedy's National Security Counsel and Defense Department leaders. Certainly, a poor communication system serving as the primary means of communication between world leaders at the brink of nuclear war would qualify as a "critical" system. This event may serve as a starting point to depict how a public service system achieves "critical infrastructure" status.

At a more pedestrian level, most people in the United States have experienced the challenge to fulfilling their daily lives when their telephone service or cell phone service is disrupted as the result of the ravages of Mother Nature. At these times it is easy to appreciate the convenience of the telephone system. The widespread loss of a public service like the telephone system is, in the early stage, an inconvenience. A more prolonged outage quickly expands from an inconvenience to an economic loss. When disrupted, public service systems such as the water supply system or the electric grid are also more easily appreciated as infrastructure that is critical to support a society. These systems are vulnerable to the ravages of Mother Nature or the sinister actions of man. Under circumstances like natural disaster, the CIP practitioner may recommend that public resilience and self-reliance for the physically and mentally able over a short period of time is a necessary element of the state infrastructure protection strategy to free government to focus on the relatively few who cannot fend for themselves, like the elderly and the handicapped.

[20] Lewis, Critical Infrastructure Protection, 29.

2. Desert Storm as a Harbinger of a Nation's Infrastructure Vulnerability

An event in 1991, almost three decades after the Cuban Missile Crisis, provides a vastly different perspective to appreciate how infrastructure becomes critical to a modern society's stability. To those who watched, the result of the U.S.-led coalition air attack on Iraq's infrastructure during Operation DESERT STORM effectively demonstrated how profoundly a modern country's national infrastructure supports its "center of gravity" and is vulnerable to fatal disruption.[21] According to a 1997 GAO report evaluating the effectiveness of the Desert Storm air campaign, the U.S. Central Command's Air Component Commander's operations order identified that the strategic air campaign would be initiated to attack, among other targets, Iraq's "command and control systems; Republican Guard forces; telecommunications facilities; and key elements of national infrastructure, such as critical LOCs [i.e., lines of communication], electric grid, petroleum storage, and military production facilities."[22] A barometer of the strategic effectiveness of the air campaign may lie in the fact that the ground war met its objectives within 100 hours. The strategic success of Operation DESERT STORM is attributed to the air attacks on Iraq's national infrastructure that supported the national government, military leadership, and defense industrial base. Once Iraq's centers of gravity were fatally disrupted, its ability to secure its sovereignty was severely taxed.

The disruption of those national infrastructure assets crippled Iraq's formerly formidable war machine. During Desert Storm, the ability of the United States military and coalition forces to completely undermine Iraq's military power by disrupting its infrastructure might be seen as a harbinger of our country's own dependence on modern infrastructure and the potential vulnerabilities of our nation's centers of gravity. The air campaign's success during Desert Storm was a public testimonial for all to see that

---

[21] "Center of gravity," in this context, is a military reference to a component or capability of an enemy that is integral to the enemy's strength to such a degree that, by destroying the component or significantly reducing the effectiveness of the capability, the enemy's ability to project offensive power or to defend itself against attack is vastly diminished.

[22] *Operation Desert Storm*.

modern infrastructure, which similarly supports most of the world's developed countries, creates a significant vulnerability to a nation's well-being.

The pace at which the federal government has been pursuing infrastructure protection over the past fifteen or more years seems to correlate with a concern for the vulnerability of the nation to a sustained military attack.

3. The Northeast Blackout Highlights the Vulnerable Power Grid

On August 14, 2003, a relatively innocuous event—as compared to Operation DESERT STORM—occurred. The event, however, highlighted the frailties of a modern power infrastructure system. That event, now referred to as the Northeast Blackout of 2003, caused the loss of electric power to parts of the northeastern and midwestern United States, as well as the province of Ontario, Canada. The widespread power blackout resulted from a power surge that stressed an Ohio power station. That surge was greatly compounded when low-hanging tree limbs shorted power lines on the Ohio electric grid. The combination of a short circuit during a power surge resulted in cascading disruptions throughout the interconnected power grid servicing the United States and Canada. A series of events linked to this outage would have remained isolated had procedures and safeguards designed to avoid power outages of this magnitude functioned effectively.[23]

This power outage is a vivid example of how a networked infrastructure is potentially vulnerable to an event triggered by man or nature. Today, regional power grids are now connected and reliant upon one another to share electricity during peaks and troughs of electric need. The power systems rely upon supervisory control and data acquisition (SCADA) technology to achieve the appropriate flow of power to meet demand across the grid. The system conserves electricity through its efficiency, but it also creates the potential for widespread failure. Our aging electric grid controlled by

[23] Minkel, "2003 Northeast Blackout."

SCADA systems that are vulnerable to computer malfunctions, combined with our nation's increased power consumption and commensurate power demand, appear to be a recipe for large-scale collapse.

As many infrastructure sectors develop more efficient delivery of goods or service through technological improvements, the infrastructure systems ineluctably become more complex. The system's complexities further multiply as infrastructure sectors become more dependent on other complex CIKR systems to function. Understanding these systems and their interdependencies is a prerequisite for state and local governments to effectively secure the assets and the systems they support.

4. Hurricane Katrina, Establishing the Limits of Vulnerability

Hurricane Katrina at many levels was an epic catastrophe. This single event certainly altered the federal government's course in managing recovery from a large-scale emergency. Katrina also exposed how Mother Nature can ravage our quality of life by eliminating our infrastructure systems. In many respects the destructive impact of Hurricane Katrina exceeded, by far, that of a nuclear bomb. Consider, for example, the swath of destruction created in the path of Katrina, beginning in Florida and extending across Alabama, Louisiana, and Mississippi—an area almost 93,000 square miles.[24] Destruction within that swath included over 1,300 deaths, with total damage estimates close to $100 billion. Nearly 300,000 residences were destroyed.[25] Within that swath of damage, 2.5 million electric-company customers reported power outages, and broadcast communications outages were realized by 50 percent of the radio stations and 44 percent of the television stations.[26] The extent and duration of these infrastructure disruptions greatly impacted the entire nation.

Although a natural disaster of this magnitude is relatively rare, Katrina clearly demonstrates the regional and national impact that the loss of service and support provided by infrastructure can mean. When considering the term infrastructure

---

[24] *Federal Response to Hurricane Katrina,* 1.

[25] Ibid., 7.

[26] Ibid., 8.

protection, there appears to be very little that man can do to protect infrastructure against this degree of wrath from Mother Nature. Yet, protection may be a misnomer, conveying an unrealistic expectation on the part of local, state, and federal security and emergency management practitioners. As futile as it may seem to protect against the extreme forces of nature, it is precisely this worst-case scenario whose effects we must prepare to mitigate.

As was indicated previously in the example of the Northeast Blackout, interdependencies within infrastructure sectors and across infrastructure sectors create potential vulnerabilities within our nation's infrastructure. Understanding those interdependencies is necessary to mitigating the effects of severe natural or man-made forces. An interesting example of this reality is shared in the *Federal Response to Hurricane Katrina*: "Federal, State and local officials responded to Hurricane Katrina without a comprehensive understanding of the interdependencies of the critical infrastructure sectors in each geographic area and the potential second and third order effects of their decisions. For example, an energy company arranged to have generators shipped to facilities where they were needed to restore the flow of oil to the entire mid-Atlantic United States. However, FEMA regional representatives diverted these generators to hospitals."[27] Without understanding the breadth and depth of an infrastructure sector, officials may make decisions that unnecessarily extend the impact of an event beyond the immediate area originally impacted.

The degree of destruction from Hurricane Katrina is thankfully a rare occurrence in this country. The degree of infrastructure loss in this example easily defines infrastructure that has achieved the status of "critical." Using this event and the others as examples to define how or when infrastructure becomes critical may convey that infrastructure is only critical when it is threatened under extreme events and when it lacks resiliency. That will be a point for consideration.

The four historical cases reviewed above demonstrate our society's reliance upon infrastructure such as the telephone system; the exponential growth in complexity of

[27] *Federal Response to Hurricane Katrina*, 61.

CIKR since the Cuban Missile Crisis; the threat to disruption of CIKR due to man-made events like military attack, as in the case of Desert Storm, or from design vulnerabilities and less than optimal maintenance, as exemplified in the Northeast Blackout; and the manner in which an extreme disaster challenges a nation's ability to maintain its people's way of life. In these examples certain infrastructure achieves critical status, but not all infrastructures are critical. Further analysis is necessary to assist a CIP practitioner to understand when infrastructure is critical and what can be done to mitigate the threat to our way of life through the loss of critical infrastructure. The analysis of federal government strategies that follows will help to further establish the federal government's parameters for infrastructure criticality and the role of state government in protecting it.

B. GOVERNMENT STRATEGY DEFINING CRITICAL INFRASTRUCTURE PROTECTION ROLES

The evolution of federal guidance relative to the definition of critical infrastructure protection is reviewed next. The following section provides examples of how different federal strategies offer varying definitions of critical infrastructure. An analysis of those strategies demonstrates that specific examples are not given as to which type of CIKR asset is considered critical and which asset is not considered critical. Federal guidance should provide specific examples of critical assets from each infrastructure sector to establish a guideline for CIP practitioners to use when determining whether an infrastructure asset achieves critical status. The overuse of criticality as an infrastructure qualifier stems from policymakers' discomfort at acknowledging that all infrastructures cannot be protected: the default is to call everything critical and treat it alike. The issue is explained well in an edition of the *Backgrounder*:

> Essentially, there is an incentive to deem infrastructure critical because of the resources that become available from such a designation. This is an inherent flaw in the NIPP, a framework which centers its approach on what it perceives as critical. Addressing this challenge will require a shared effort between the private sector and the federal government, as well as hard choices, to disaggregate what is "critical" (essential for

> sustaining and supporting Americans' daily lives) from what is "dangerous" (e.g., chemical facilities) but not necessarily critical.[28]

Without specific criteria for what is critical, including an explanation of how and why an asset is believed to be critical, CIP practitioners may be influenced to label an asset as critical solely to receive federal grant funds to enhance the protection of that asset. We will review different federal strategies that provide ambiguous definitions of infrastructure criticality.

According to a Congressional Research Service report for Congress, a 1983 Congressional Budget Office report qualifies infrastructure as that which is "directly critical to the nation's economy." The report further lists examples of infrastructure, including "highways, public transit systems, wastewater treatment works, water resources, air traffic control, airports and municipal water supply."[29] By 1996, government interest and its developing understanding of the complexity of critical infrastructure protection is evident in the evolving descriptions of critical infrastructure. In that year, the opening sentence of E.O. 13010, "Critical Infrastructure Protection," describes critical infrastructure as being "so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."[30] The executive order listed telecommunications, electrical power systems, gas and oil storage, banking and finance, transportation, water supply systems, emergency services, and continuity of government as inclusive of critical infrastructure. The executive order also broadly identified the threats to infrastructure as falling into two categories: either "physical threats" or "cyber threats."[31] That description of critical infrastructure is certainly subject to individual interpretation as to what "vital" means and what constitutes "a debilitating impact." How, then, should a state or local government

---

[28] McNeil and Weitz, "How to Fix," 4.

[29] "Critical Infrastructure," 2.

[30] Executive Order 13010, 1.

[31] Ibid, 1.

interpret the federal guidance in order to protect appropriate infrastructure in its jurisdiction? Analysis of successive federal strategies will demonstrate the evolving federal definition of "critical" infrastructure.

Within two years, the Presidential Decision Directive 63 described critical infrastructure as "those physical and cyber-based systems essential to the minimum operations of the economy and government."[32] The obvious focus of PDD 63 was directed to the "cyber-based" vulnerability of critical infrastructure:

> Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked.[33]

In two short years, our national leaders were learning just how interdependent our infrastructure systems had become and, subsequently, how apparently frail the infrastructure was due to cyber threats. As our national leaders expanded the parameters of what constitutes critical infrastructure and its potential vulnerabilities, state governments remained challenged to understand their role in protecting those assets.

The USA Patriot Act, written in the shadow of the 9/11 terror attacks, describes critical infrastructure and key resources (CIKR) as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health, or any combination of those matters."[34] This broad definition, inclusive of many entities and assets, only expands the spectrum of assets that may achieve critical status. Without specific examples of critical assets, state government remains challenged to gauge which infrastructure is actually critical.

---

[32] White House, *Protecting America's Critical Infrastructure*, 1.

[33] Ibid., 1.

[34] USA Patriot Act, Section 1016(e).

Within two years, the release of the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, in February 2003, identified the critical infrastructure protection issue, explaining,

> The facilities, systems, and functions that comprise our critical infrastructures are highly sophisticated and complex. They include human assets and physical and cyber systems that work together in processes that are highly independent. They also consist of key nodes that, in turn, are essential to the operation of the critical infrastructures in which they function.[35]

This strategy acknowledges the expanding complexity of CIKR, the interdependencies and the breadth of assets that make up CIKR, and it expands the description of critical infrastructure to include human assets and cyber systems while publicly acknowledging the existence of "key nodes." Yet, again, federal guidance only expands the number of assets potentially falling into the spectrum of critical infrastructure. Interestingly, the strategy remains focused on the threat to CIKR from terrorism. Of course these strategies were written with the attacks of 9/11 relatively fresh in people's minds and still years before the impact of Hurricane Katrina altered the federal strategic view of CIKR.

The 2009 National Infrastructure Protection Plan (NIPP) represents a significant evolution from the government's view of infrastructure evident in the 1980s. The 2009 edition of the NIPP demonstrates a refined federal government understanding of the CIKR protection issue. However, in the glossary of key terms of the 2009 NIPP, the definition of critical infrastructure remains consistent, almost to the word, to that in the Patriot Act.[36] In the body of the 2009 NIPP, CIKR is broadly qualified:

> Attacks on CIKR could significantly disrupt the functioning of government and business alike and produce cascading effects far beyond the targeted sector and physical location of the incident. Direct terrorist attacks and natural, manmade, or technological hazards could produce

[35] White House, *Physical Protection*.

[36] *NIPP*, 109.

> catastrophic losses in terms of human casualties, property destruction, and economic effects, as well as profound damage to public morale and confidence.[37]

Based on this description, one can infer what assets meet those qualifications. There remains a need for a more definitive description, with examples, of what constitutes CIKR.

Solid research is needed to support the criterion that defines the criticality of infrastructure. Eliminating ambiguity as to what is critical will minimize the CIP practitioner's burden of validating what is or is not a critical asset to a politician looking to spread some "pork." In the absence of specific criteria to designate CIKR as critical, a state CIP practitioner should search for and read as much research material on this subject as is possible in order to develop a learned opinion of what infrastructure is truly critical.

Having reviewed the issue surrounding the definition of what is critical, we will begin the analysis of state government's role in CIKR protection. The NIPP suggests that, in order to protect CIKR across the nation, establishing partnerships between federal government, state government, and the private sector is important. In order to be a good partner, one must know who his partners are, their capabilities, and their motivations. In that light, the next chapter will examine the roles performed by two of the significant federal partners with which state governments will interact with to protect CIKR: the Department of Homeland Security and the Department of Defense.

[37] *NIPP*, 1.

THIS PAGE INTENTIONALLY LEFT BLANK

III. THE FEDERAL GOVERNMENT'S STAKE

The federal government has assumed responsibility for protecting CIKR throughout the nation. That is a broad mandate that is shared by numerous federal agencies, as identified in Figure 1. Of the federal agencies listed in Figure 1, state government infrastructure protection practitioners will predominantly interact directly with the Department of Homeland Security (DHS) and the Department of Defense (DoD). The state government infrastructure protection practitioner, as a partner in the CIKR protection effort, should understand their partners' infrastructure protection mandate. The state should also understand each of their federal partners' CIP roles in order to more effectively support the federal effort, to coordinate state and local protection efforts, to avoid duplicating efforts with the federal government, and to gauge which protection efforts may not be covered in their state by the federal government. In the event that the federal government is deficient in fulfilling its CIP role in a given state, that state may elect to fill the federal void and assume the federal CIP responsibility. A state's election to fill a void will certainly impact the composition of that state's CIP program.

This chapter provides an overview of the CIP roles of the DoD and the DHS. Background information about both federal departments' CIKR protection mandate will also provide basic insight into federal CIP expectations for the state government. This author rationalized the state's need to understand the federal roles based upon a concept in military planning: in order to achieve proper coordination and unity of effort, entities tasked within a plan or strategy should know the roles and responsibilities of the tasked and supporting units at echelons above and below them. Similarly, in the national CIP effort, each of the entities tasked to protect CIKR should know its partners' tasked roles and capabilities.

A. THE SECRETARY OF THE DEPARTMENT OF HOMELAND SECURITY

The Department of Homeland Security was established under the Homeland Security Act of 2002. The creation of the DHS consolidated numerous disparate federal agencies under the control of the Secretary of Homeland Security. By virtue of the new department's broad homeland security mission, the Secretary of Homeland Security was also tasked to be the single individual responsible to coordinate the federal government's CIKR protection effort. Homeland Security Presidential Directive 7 (HSPD-7) issued December 17, 2003, establishes the mandate of the Secretary of Homeland Security with respect to CIKR protection. As stipulated in HSPD-7:

> In carrying out the functions assigned in the Homeland Security Act of 2002, the Secretary shall be responsible for coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States. The Secretary shall serve as the principal Federal official to lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, State and local governments, and the private sector to protect critical infrastructure and key resources. Consistent with this directive, the Secretary will identify, prioritize, and coordinate the protection of critical infrastructure and key resources with an emphasis on critical infrastructure and key resources that could be exploited to cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction.[38]

The above guidance outlines the broad responsibilities of the Secretary of Homeland Security. In order to discharge those duties, the Department of Homeland Security created directorates with commensurate tasks to execute the duties assigned to the secretary. One of those DHS directorates is the National Programs and Protection Directorate. Assigned within the National Programs and Protection Directorate is the Office of Infrastructure Protection, which bears the primary responsibility to carryout the Department of Homeland Security's CIKR protection mission.

[38] White House, HSPD-7.

1. Office of Infrastructure Protection

Within the Office of the Under-Secretary for National Protection and Programs is the Office of Infrastructure Protection (IP), which is designated as the lead within the Department of Homeland Security to coordinate the national effort to protect critical infrastructure. According to the DHS website, the NIPP is the guiding document for the IP. The Office of Infrastructure Protection is comprised of the following seven divisions:

- Contingency Planning and Incident Management Division (CPIMD);
- Infrastructure Analysis and Strategy Division (IASD);
- Infrastructure Information Collection Division (IICD);
- Infrastructure Security Compliance Division (ISCD);
- Partnership and Outreach Division (POD);
- Protective Security Coordination Division (PSCD); and
- Sector Specific Agency Executive Management Office (SSA EMO).

Of the divisions within the Office of Infrastructure Protection, the Protective Security Coordination Division is one that the state or local infrastructure protection entities will regularly interact with. Each state has at least one protective security advisor (PSA) who is assigned to the PSCD as a liaison to a given state. The PSA should provide the conduit between the state or local government entity and DHS for federal guidance and resources with respect to CIKR protection.

Independent of a PSA, the state CIP practitioner should establish working relationships with DHS representatives in each of these seven divisions in order to receive additional federal support and guidance. Justification for a state CIP practitioner to develop secondary relationships within the seven divisions is evidenced in a 2010 GAO report. That report questions the effectiveness of the PSA program to disseminate recent IP guidance to state governments and the private sector with respect to developing resilient capacity, the core principle espoused in the 2009 NIPP.[39] That diminished

[39] "Critical Infrastructure Protection."

capacity brings into question the effectiveness of the PSAs in other CIKR matters. The lack of PSA effectiveness in this core area indicates to this author that a state CIP practitioner ought to be prepared within his state jurisdiction to facilitate the functions tasked to the PSA.

The IP website lists five of the office's goals, which are:

- Goal 1: "Understand and share risk and other information about terrorist threats and other hazards to the nation's critical infrastructure and key resources."
- Goal 2: "Build and sustain effective CIKR partnerships and coordination mechanisms."
- Goal 3: "Build and implement a sustainable, national CIKR risk management program."
- Goal 4: "Ensure efficient use of resources for CIKR management."
- Goal 5: "Provide a foundation for continuously improving national CIKR preparedness."

The DHS website elaborates on each of these goals. The amplification of the goals on the website better defines the critical infrastructure protection objectives of DHS and is a good guide to help state governments understand how DHS intends to achieve CIKR protection nationally. Some excerpts are included here to explain the CIKR protection effort and as a reference later to gauge whether the goals are being met or whether the information is simply public relations rhetoric.

The objective of Goal 1, "to understand and share risk and other information about terrorist threat and other hazards," focuses a portion of the effort toward information sharing—an effort that has proven to be a challenge to the overall homeland security mission. This goal identifies the DHS position that:

> CIKR protection cannot be effective in an atmosphere of limited information. Working collaboratively with our security partners, The Office of Infrastructure Protection collects and maintains the widest possible spectrum of data related to the nation's critical infrastructures/key resources. This data is acquired from our security partners—i.e., regional entities and centers; federal, state, local, tribal and territorial governments; and the private sector—and drawn from information contained in the

> Sector-Specific Plans (SSPs) and the National and Sector CIKR Protection Annual Reports, among various other sources, to include periodic data calls. [40]

Goal 1 broadly describes the groups that the federal government believes are its partners in the realm of sharing CIKR information and threat and warning information. However, are the appropriate people in each of these partnerships receiving the information, and does the information shared provide value to further the protection effort?

The objective of Goal 2, to "build and sustain effective CIKR partnerships and coordination mechanisms," is an obvious objective of a protection effort. Partnerships and coordination are not novel concepts in the homeland security realm. Goal 2 states that "effective critical infrastructure and key resources protection requires teamwork, communication, collaboration and coordination among all security partners." Of interest is DHS's stated perspective: "The Office of Infrastructure Protection's ultimate goal is for each element—be it at the regional, state, local, tribal or territorial level—to have the ability to conduct its own assessments and analysis, coordinate and collaborate with every other element, and share information across all strata of the public and private sectors." This seems to be an ambitious, possibly utopian goal. However, it is essential in order to relieve the federal government of the burden to inventory, assess, and coordinate the protection of the nation's entire infrastructure. The enduring challenge in fulfilling this goal is for the federal government to engender the will and commitment from all of its identified partners. The quality of the assessments and analysis is critical. Deficient assessments and analysis based on faulty information will be useless. Ultimately, this is a worthy goal but one that will take a long-term commitment from all the partners to achieve.

To leverage the capabilities of its partners and to engender their buy-in, the DHS has created Sector Coordinating Councils (SCC) and Government Coordinating Councils (GCC). The DHS website describes the SCCs as "self-organized, self-run and self-

[40] Department of Homeland Security. Office of Infrastructure Protection.

governed organizations that represent a spectrum of key stakeholders within a sector."[41] The GCCs are the government's peers to the SCCs. The GCCs and SCCs coordinate CIKR protection issues across sectors. Two groups that represent the government interests with the SCCs are the Federal Senior Leadership Council (FSLC) and the State, Local, Tribal and Territorial Government Coordinating Council (SLTTGCC).[42] The SLTTGCC is the group with which state and local CIKR protection practitioners should develop a relationship in order to gain understanding and remain connected to relevant issues in the CIKR protection arena.

The objective of Goal 3 is to "build and implement a sustainable, national CIKR risk management program." The tone of the 2009 NIPP—to "manage risk" as opposed to "securing" infrastructure—may amount to pure semantics, but, given the nature of our free society, the vastness of our geography, and the commensurate breadth and complexity of the supporting infrastructure, managing risk to CIKR sectors seems to be a more achievable objective than securing and protecting all of the CIKR. The issue of CIKR risk management will be addressed later in this thesis. However, the role of IP in managing risk will be reviewed now.

According to their website, DHS specifies that IP will establish a program to assess risk, initiate protective actions, ensure effective incident response, and prioritize resource investment in a transparent and strategic manner. Risk analysis and risk management is an area that may be foreign to state CIP practitioners. Knowledge of IP's risk management roles will enable the state CIP practitioner to better understand what he should do to support the federal risk management effort. The DHS website establishes that "incident management is a key component of the Office of Infrastructure Protection's risk management framework."[43] Philosophically, IP recognizes that effectively managing a critical incident translates into diminishing protracted risk. Managing a critical incident is an area where state and local emergency managers should understand the roles they play and help greatly to manage risk.

---

[41] Department of Homeland Security. Office of Infrastructure Protection.

[42] Ibid.

[43] Ibid.

The fourth goal of IP, to "ensure efficient use of resources for CIKR risk management," incorporates the objective of the NIPP to invest protection resources in the areas of highest priority. Coordinating the effort to prioritize CIKR protection efforts and resources is an unenviable task. According to the DHS website, "the Office of Infrastructure Protection and its security partners collaborate to define risk management needs, establish criteria to rank CIKR priorities, share risk information, and optimize finite resources. These determinations, developed through review and coordination of the 17 Sector Specific Plans and the Sector CIKR Protection Annual Reports in addition to other sources, provide the foundation for recommendations and guidance as to how federal, state, local and private sector resources are used to best address sector and national risk."[44] The state CIP practitioner should know whom to channel their protection recommendations to in their state for inclusion in the national CIKR Protection Annual Report. In the areas affected by this goal, the state CIP practitioner should know the concepts behind risk analysis and, armed with that knowledge should hold IP to its task of coordinating the efficient use of resources by advocating their jurisdiction's CIKR vulnerabilities and risk and advocating their state's requirements to mitigate those vulnerabilities and commensurate risk.

The fifth and final goal, to "provide a foundation for continuously improving national CIKR preparedness," equates to the mantra of any professional to continuously improve. IP intends to achieve this goal through the development and exercise of continuity of operations (COOP) plans and by partaking in federal, state, and local government and private-sector exercises and training opportunities. IP tasks itself to guide state and local government and private-sector incident management exercises to factor the National Response Framework into their planning efforts. An interesting component of Goal 5 is the inclusion of efforts to increase a given community's awareness of its responsibility to protect its CIKR from all hazards. An important element of this goal is IP's effort to develop "national-level critical infrastructure/key resources education, training and exercise programs" and "interactive Web- and classroom-based critical infrastructures/key resources awareness training programs in partnership with the

[44] Department of Homeland Security. Office of Infrastructure Protection.

Federal Emergency Management Agency (FEMA) and Federal Law Enforcement Training Center (FLETC)."[45] Providing professional development education opportunities in the realm of CIKR assessment, and protection is critically important to the success of the nation's CIKR protection effort. However, the quality of instruction and the content of material from the FEMA and FLETC courses must be superior in order to avoid sending poorly trained and ill-informed practitioners to protect our nation.

A review of IP's goals provides a wealth of insight for state and local governments with respect to their role in CIKR protection in the eyes of DHS. The information in the goals can be used as a reference guide to important subjects and coordinating entities regarding CIKR protection.

2. Homeland Infrastructure Threat and Analysis Center

The Office of Infrastructure Protection has identified understanding and sharing CIKR risk and hazard information as Goal # 1. Referencing the DHS website the following information was gleaned to provide an overview of the Homeland Infrastructure Threat and Analysis Center (HITRAC), an important mechanism to achieve IP's Goal #1. Within HITRAC analysts from IP and the Office of Intelligence and Analysis work together to provide actionable intelligence that is relevant to infrastructure protection. "Actionable intelligence" is the popular vernacular for specific and validated intelligence that allows security entities to organize relevant and effective operations. Whether or not intelligence producing entities, such as HITRAC, achieve that intelligence standard is open to debate. Articles regarding information sharing will be analyzed later in this thesis to gauge how well the intelligence and risk analysis needs of CIP partners are being met.

HITRAC is tasked to research and produce infrastructure threat analysis that will support its customers' ability to develop CIKR threat mitigation strategies. The threat analysis evaluates enemy tactics and capabilities to identify threats to assets within critical infrastructure sectors. The HITRAC concept established a consolidated group of

[45] Department of Homeland Security. Office of Infrastructure Protection.

experienced and informed analysts who should be able to focus energy toward understanding threats to CIKR sectors and producing accurate assessments of what constitutes a relevant threat. It is probably fair to state that their combined expertise would exceed the capability that any single state fusion center could direct toward analyzing a CIKR sector. Assuming their capability is strong and their analysis is relevant, HITRAC is a valuable resource for a state or local government's CIP program. As a component of their charter, HITRAC is tasked to produce state critical infrastructure threat assessments with a given state's local intelligence input. HITRAC should be challenged by state CIP practitioners to produce CIKR intelligence specific to their needs.

The complexity of modern CIKR could challenge state and local analysts to produce relevant risk analysis. Fortunately, HITRAC is also tasked to provide CIKR risk analysis to federal, state, and local government and the private sector. Subject matter experts at HITRAC evaluate cyber threats within and across sectors, assist government entities to prioritize CIKR assets within their jurisdiction, and develop CIKR modeling and simulation scenarios to assist entities to understand whether a presumed risk in fact presents a threat to CIKR.

HITRAC's task to produce intelligence-based infrastructure threat analysis underpins DHS's overall effort to protect CIKR and supports the critical infrastructure protection practitioners at the federal, state, local, and private-sector levels. HITRAC's products are intended to directly support threat mitigation strategies and investment decisions of DHS's CIP partners, inform their partners about physical and cyber threats to critical infrastructure, and educate their partners about enemy tactics and capabilities.

HITRAC is tasked to produce tailored threat assessments in conjunction with state and local homeland security professionals. State and local CIP practitioners should be fully engaged with HITRAC to provide local information to HITRAC analysts and challenge them to provide relevant threat analysis. HITRAC should regularly provide state critical infrastructure threat assessments, host weekly threat teleconferences and regional threat conferences, provide threat briefing support, and provide critical infrastructure threat analysis that addresses specific CIKR sectors and cyber threat

analysis. Cyber threat is the burgeoning concern for CIP practitioners and one that requires experienced, knowledgeable analysts to provide accurate threat and risk assessments.

HITRAC also supports a number of programs, including its infrastructure risk analysis partnership program, which assists state and local practitioners to evaluate risk. A state CIP program should be actively engaged with HITRAC to develop as much understanding of the threat and risk to CIKR in the jurisdiction as is practical.[46]

3. Federal Emergency Management Agency

Many people appreciate the role of the Federal Emergency Management Agency (FEMA) when it responds to assist communities to recover from large-scale disasters. Not as well appreciated is the significant role that FEMA plays in preparing our nation to secure critical infrastructure. In the scope of current infrastructure assurance, CIKR security is achieved through a full spectrum of actions, including preparedness, protection, response, recovery, restoration, resilience, and continuity of operations. The concepts listed above are understood by state and local emergency managers, firefighters, and police officers due to training, exercising, and when necessary responding to natural or man-made disasters. State and local first-responders developed these capabilities prior to 9/11 through years of interaction with FEMA. This understanding and established relationships can be exploited to help the state and local infrastructure protection practitioners and leaders to understand how those same skill sets should be further developed and applied proactively to infrastructure protection.

When released in May of 1998, PDD 63 established FEMA as the lead federal agency for emergency fire services and continuity of government.[47] However, under the current NIPP FEMA is not identified specifically as a sector specific agency or as a lead agency to coordinate security for any of the CIKR sectors. However, the activities that

[46] Department of Homeland Security. Homeland Infrastructure Threat and Analysis Center.

[47] White House, *Protecting America's Critical Infrastructure*.

state and local governments have been directed to accomplish and the capabilities that they have developed to achieve emergency response with FEMA will be effective to meet current DHS CIKR directives.

The aftermath of Hurricane Katrina certainly motivated state and local governments to sharpen their capacity to respond to major disasters and appreciate that they need to continuously improve their response capability. In a similar light, state government should strive to better understand critical infrastructure vulnerability issues and to better appreciate the proactive role necessary to avoid infrastructure disaster. As seen in the response to Hurricane Katrina, FEMA plays a huge role in recovering from disaster by restoring the critical infrastructure to deliver services to the public.

A FEMA-coordinated federal response is achieved through the mobilization and deployment of emergency support functions (ESF). There are 15 ESFs, representing a variety of capabilities, for example, transportation, engineering, communication, public health, search and rescue, and firefighting. Each of the ESFs has an assigned ESF coordinator. The ESF coordinator is a federal agency; for example, the Department of Transportation is the ESF coordinator for ESF #1, Transportation, and the Department of Defense (US Army Corps of Engineers) is the federal coordinator for ESF #3, Public Works and Engineering.[48] It should be understood that federal assistance to state and local governments is regulated under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act) that requires a presidential declaration of disaster or emergency within an area before FEMA can dispense funds or equipment on behalf of the federal government. The incident must clearly exceed a state and local government's capacity to manage the event in order for the president to make a declaration.[49]

As identified in the NIPP, "the NIPP risk management framework recognizes and builds on existing public and private sector protective programs and resiliency strategies in order to be cost effective and to minimize the burden on CIKR owners and

[48] National Response Framework, 58.

[49] Ibid., 40.

operators."[50] It makes sense to leverage the existing capabilities that state and local governments and the private sector have developed for disaster response. The disaster response capabilities are identified in the National Response Framework (NRF). The NRF is an important document for state and local CIP practitioners to digest because it outlines the roles of the federal, state, and local governments, as well as the private sector, in disaster preparedness, response, and recovery. "The NIPP, The National Preparedness Guidelines (NPG) and the National Response Framework (NRF) together provide a comprehensive, integrated approach to the homeland security mission."[51] Many public/private partnerships were established through historical efforts of FEMA well before the NIPP was a strategy. The NIPP identifies that, "NIPP partnerships and processes provide the foundation for the CIKR dimension of the NRF, facilitating threat and incident management across a spectrum of activities, including incident prevention, response and recovery."[52]

The NRF identifies "layered mutually supporting capabilities" as a doctrinal approach to national emergency response that should be adopted in steady state critical infrastructure protection. "Communities, tribes, States, the Federal government, NGOs and the private sector should each understand their roles and responsibilities and compliment each other in achieving shared goals. Each governmental layer plays a prominent role in developing capabilities needed to respond to incidents."[53] Certainly, emergency managers, firefighters, and police understand how to complement FEMA's role in responding to large-scale emergencies. In these instances, the focus of the state and local government is to restore the delivery of goods and services.

The National Response Framework (NRF) is an important federal strategy that should be understood by state and local first responders, critical infrastructure protection practitioners, and their leadership. The NRF is a good guide for identifying the

---

[50] *NIPP*, 2009, 1.

[51] Ibid., 5.

[52] Ibid.

[53] *National Response Framework*, 4.

relationships and integration necessary for federal, state, and local CIP practitioners to posture their agency to succeed in infrastructure protection.

4. Sector Specific Federal Agencies

As identified earlier, the task of protecting the nation's critical infrastructure is vast and complex. Although the Department of Homeland Security is tasked to coordinate the overall CIKR effort, the responsibility for managing aspects of that effort is shared across many agencies of the federal government. For the purpose of the national CIKR protection effort, many federal agencies have been assigned responsibility to direct their support to a particular critical infrastructure sector. HSPD-7 identifies the federal departments and agencies to support a particular infrastructure sector. According to NIPP, "the SSAs are responsible for working with DHS and their respective GCC (Government Coordinating Council) to: implement the NIPP sector partnership model and risk management framework; develop protective programs, resiliency strategies, and related requirements; and provide sector-level CIKR protection in line with the overarching guidance established by DHS pursuant to HSPD-7."[54]

The development of Sector Specific Plans (SSP) is a significantly important task assigned to the SSAs and results in a product that state CIP practitioners should be aware of. SSAs coordinate the development of a security plan for each of the critical infrastructure sectors in conjunction with the private-sector infrastructure asset owners and operators. Many of the SSPs are classified "For Official Use Only" and are available through the Protective Security Advisor assigned to the state. State and local practitioners should review the SSPs relevant to infrastructure in their jurisdiction to gain a better understanding of what is tasked in the security plan and to appreciate what is not in the plan. The plans are written from a national-level perspective and therefore do not task specific states; however, the general guidance will provide the reader with a better appreciation for issues within the sector and the general tasks recommended to better secure that sector.[55]

---

[54] *National Infrastructure Protection Plan*, 18.

[55] This observation is based on the author's two years of experience working in the Commonwealth of Massachusetts Fusion Center on critical infrastructure protection.

This author reviewed many of the publicly available SSPs. Of the SSPs reviewed each simply reiterates guidance from the NIPP with language relative to its infrastructure sector. For example, the SSPs for the water sector and the critical manufacturing sector each reads like the regurgitation of NIPP guidance cloaked in that sector's parlance. There is very little specific guidance detailing how to provide for a particular sector's protection.

An additional benefit of the SSA to the state CIP practitioner is through the SSA's ability to influence and encourage private-sector businesses within a given sector to share information among their potential competitors and with the government. As often stated, 85 percent of the critical infrastructure in this country is owned by the private sector, which often views its internal information as proprietary and sensitive to its ability to maintain an edge over the competition. The fact that many of these privately owned businesses share security and other information among their competitors and with the government is significant.

Direct interaction with the SSAs might best be served by a state's homeland security advisor, as opposed to an individual member of a state government's Infrastructure Protection Unit. Absent direct interaction by the state HLS advisor, indirect inquiries of the SSA can be made through the state PSA.

Figure 1 lists the SSAs and their commensurate CIKR sectors.

Sector-Specific Agency	Critical Infrastructure and Key Resources Sector
Department of Agriculture[a] Department of Health and Human Services[b]	Agriculture and Food
Department of Defense[c]	Defense Industrial Base
Department of Energy	Energy[d]
Department of Health and Human Services	Healthcare and Public Health
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Water[e]
Department of Homeland Security *Office of Infrastructure Protection*	Chemical Commercial Facilities Critical Manufacturing Dams Emergency Services Nuclear Reactors, Materials, and Waste
Office of Cybersecurity and Communications	Information Technology Communications
Transportation Security Administration	Postal and Shipping
Transportation Security Administration *United States Coast Guard*[f]	Transportation Systems[g]
Immigration and Customs Enforcement, Federal Protective Service	Government Facilities[h]

Figure 1. National Infrastructure Protection, 2009

B. THE DEPARTMENT OF DEFENSE AS A SECTOR SPECIFIC AGENCY

With respect to the national critical infrastructure protection effort, the Department of Defense is identified as the sector specific agency to coordinate the

securing of the defense infrastructure sector (DIS), which includes the defense industrial base (DIB). The overall DIS is divided into segments for which lead agents are tasked to oversee their security. The DoD's role in infrastructure protection was selected for analysis for several reasons: it has a history of conducting vulnerability analysis of infrastructure, the DIS is inclusive of a broad scope of assets residing within state jurisdictions, and DoD is perceived as having an obvious capacity to provide security for our nation's CIKR. As stated, DoD's task to coordinate security of the DIS dictates that the DoD will be engaged with many CIKR-sector asset owners and state government.

It is important to understand what the DIB is and to understand the SSA mission with respect to the DIB. A Government Accountability Office report describes the DIB as "a global network of critical physical and cyber infrastructure to project, support, and sustain its (i.e., DoD's) forces and operations world-wide."[56] That description provides a general perspective of the potential importance of the DIB but does not definitively describe the type of physical and cyber assets that compose the network. The website for the Office of the Under Secretary of Defense for Policy further describes the DIB as "the DoD, U.S. Government, and private-sector worldwide industrial complex with capabilities to perform research and development, design, produce, deliver and maintain military weapon systems, subsystems, components, or parts to meet military requirements. The DIB includes hundreds of thousands of domestic and foreign entities and their subcontractors performing work for DoD and other federal agencies."[57] This explanation provides more than enough information to appreciate that elements of the DIB are interwoven throughout the nation and any given state.

A GAO report describes the importance of the DIB explaining that "the incapacitation, exploitation, or destruction of one or more of its assets would seriously damage the DoD's ability to carry out its core-missions." Considering that reality it should be noted that specifically identifying assets comprising the DIB may violate classified information security. The Assistant Secretary of Defense for Homeland Defense and America's Security Affairs (HD&ASA) manages the Defense Critical

[56] Government Accountability Office, "Defense Critical Infrastructure."

[57] Office of the Under Secretary of Defense for Policy.

Infrastructure Program (DCIP), tasked to secure defense infrastructure.[58] The Assistant Secretary of Defense for Homeland Defense and America's Security Affairs guides the DoD's effort to secure the DIB, develops policy to that end, and advocates for resources to accomplish the mission. The DoD has the responsibility to identify, assess, prioritize, remediate threats, and protect defense critical infrastructure. As the sector specific agency for the DIB, DoD has the responsibility to "collaborate with all relevant federal departments and agencies, state and local governments, and the private sector, including key persons and entities in their infrastructure sector, conduct and facilitate vulnerability assessments of the sector, encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources; and support sector coordinating mechanisms."[59]

The Department of Defense directive providing guidance for the DIB protection effort is 3020.40. That directive stipulates that it is DoD policy that the risk management of defense critical infrastructure (DCI) shall be accomplished with other federal departments and agencies; state, local, regional, territorial, and tribal entities; the private sector; and foreign countries, as appropriate. It also states that DoD will identify, prioritize, assess, mediate, and protect DCI, working with federal, state, and local governments and the private sector to accomplish those tasks. The protection tasks identified under 3020.40 are essentially identical to those identified for other federal entities acting as an SSA for other critical infrastructure sectors. How does the DoD achieve strategic objectives such as risk management with the state and local entities?

Further guidance in DoDD 3020.40 recognizes that the primary DoD interaction with state and local government may be with a local base or installation commander. The directive establishes that the heads of the DoD components, Defense Infrastructure Sector Lead Agent (DISLA) and the chief of the National Guard Bureau, "establish the necessary lines of communication and promote information sharing with each other and with federal departments and agencies; state, local, regional, territorial, and tribal entities; the private sector; and foreign countries as appropriate." The directive also tasks these

[58] Government Accountability Office, "Defense Critical Infrastructure."

[59] Office of the Under Secretary of Defense for Policy.

entities to coordinate or consult, as appropriate, with the above-listed entities to implement a standardized process for DCI and inter- and intra-dependency identification based upon DoD missions. Given this guidance it is quite likely that the state and local CIP practitioner would be interacting with members of his state's National Guard forces.[60] These entities are instructed to conduct assessments of the threats, hazards, vulnerability, and risk to DoD-owned defense critical infrastructure. DODD 3020.40 tasks the chief of the National Guard to "support the organization and training of assessment teams to provide a standardized method to assess vulnerabilities, including physical, personnel, and cyber issues, and consequences throughout the DIB."[61] It is in this area that state and local governments could target working with the National Guard.

Considering the nature of the DIB, one might expect that the National Guard has assumed a significant role in the nation's critical infrastructure protection effort. The National Guard website highlights the fact that the National Guard Bureau conducts CIKR assessments in coordination with the Defense Contract Management Agency, designated as the lead agency for the DIB, and with DHS. The National Guard provides three nine-person teams made up of Army and Air National Guard personnel. One of each of the three teams is from each of the following states: Colorado, New York, and West Virginia. The teams conduct "all-hazard, vulnerability assessments" on behalf of the Assistant Secretary of Defense. The teams support DHS requests for three types of assessments: 1) site-assisted visit, 2) buffer zone protection technical assist or buffer zone protection workshop and 3) utilizing the Computer Based Assessment Tool (CBAT).[62]

With that overview of two significant federal partners established, it is necessary to review the role of the most significant partner in the national CIP effort. The private sector, as the owner and operator of the predominant percentage of CIKR in this country, is the most significant partner. Understanding the private-sector perspective to CIKR protection is the key to success. The next chapter will provide some insight into the private sector perspective of CIP.

---

[60] Department of Defense Directive 3020.40.

[61] Ibid., 14.

[62] *The National Guard's Role in Homeland Defense*.

IV. THE PRIVATE SECTOR AS PARTNER

This chapter will analyze the debate regarding the private sector as a stakeholder in the CIKR protection effort and address how the state CIP practitioner can partner with the private sector to enhance CIKR protection. Through my research I have identified five proposed areas where the private sector's involvement can affect the posture of the national CIKR protection effort. The five areas are addressed as subsections of this chapter:

- The federal government's value proposition;
- Managing for reliability;
- Network security;
- The insurance option; and
- The issue of trust.

Each of the five areas will be analyzed to establish the conceptual benefit of a private-sector role in the national CIP effort and to identify where the federal government and the state CIP practitioner can facilitate the public/private partnership to enhance CIKR protection.

As addressed earlier, the private sector is identified as having control of 85 percent of the nation's CIKR. The genesis of that percentage is nebulous but commonly repeated, and it is apparently generally accepted as a fact based on its repeated mention throughout relevant literature. However, at least one voice challenges that oft-repeated statistic, and it is important to note because of the effect that statistic has on framing the private sector's role in CIP. Dr. Bellavita's analysis of the impact of that statistic, which he qualifies as a proverb in his article "How Proverbs Damage Homeland Security," is an important critique of the CIKR protection effort and challenges the status quo thinking within homeland security. Dr. Bellavita identifies the following four reasons why the 85-percent proverb damages the CIKR protection effort:

- It gives the impression that we know more than we do when it comes to critical infrastructure;
- It creates a false image about the power relationships between the public and private sectors;
- It distorts normative understanding about roles and responsibilities;
- It constrains discussions about policy options.[63]

Dr. Bellavita's thoughts on this subject will be considered throughout my analysis of the private-sector role in CIKR protection, and they influence my analysis throughout this thesis.

Despite the lack of validation of the 85-percent proverb, upon consideration of different infrastructure sectors such as electric power, petroleum, communication, finance, or rail, which are predominantly privately owned, one can begin to fathom that the majority of CIKR in this country may be owned or controlled by the private sector. Accepting that the private sector controls a majority of the nation's infrastructure qualifies the private sector as a necessary participant to secure CIKR sectors. To maximize the national CIP effort, inclusion of the private sector in the nation's protection effort is paramount. It will not be possible to effectively secure CIKR without the cooperation and involvement of the private sector, the federal government, and state governments.

What, then, is the private sector's role in CIP? This chapter will attempt to address some of the roles that private industry can undertake to fulfill federal government expectations, support state government CIKR protection efforts, and assure delivery of services.

A. THE FEDERAL GOVERNMENT'S "VALUE PROPOSITION"

"The Value Proposition" is addressed in the first pages of the NIPP. That value proposition is described as a public-private partnership laying the foundation for prevention, response, mitigation, and recovery.

[63] Bellavita, "How Proverbs Damage."

1. The Government's Interest in the Private Sector's Value

The NIPP proposition recognizes the value of industry capabilities such as:

- Their "understanding of CIKR assets, systems, networks, and facilities and other capabilities through industry ownership and management;"
- Their "ability to reduce risk and respond to and recover from incidents;"
- Their "ability to innovate;" and
- Their "robust relationships that are useful for sharing and protecting sensitive information regarding threats, vulnerabilities, countermeasures, and best practices."[64]

The NIPP wisely acknowledges that these industry capabilities are of value to the government, but what value does the private sector realize in its relationship with government in these matters?

For the most part, private-sector involvement to fulfill this national strategy relies on its altruism. Stephen E. Flynn, in his article "The Brittle Superpower," questions whether private industry will independently invest in significant infrastructure protection measures as envisioned in the NIPP. Flynn comments that "critical infrastructure protection and emergency preparedness will not happen if left solely to the marketplace."[65] Similarly to Dr. Lewis, Flynn believes that state and local involvement in the protection relationship alone will not suffice, and he contends that the effort should be led by the federal government. Flynn also argues that the federal government's attention is directed elsewhere, and he questions whether the federal government is sufficiently engaged in the CIKR protection effort to achieve the NIPP goals. Is there a clear leader in the national CIKR protection effort? Is industry better positioned to lead the national CIKR protection effort? Maybe the public-private CIP partnership should be led similarly to the national Incident Command System's doctrine of unity of command where, for example, in the CIP partnership each partner has an equal say in the protection effort. That unified leadership concept will be recommended later in this thesis. We will now

---

[64] *NIPP*, 2009, 5.

[65] Flynn, "Brittle Superpower," 27.

look at some enticements for the private sector to participate in the public-private partnership. The enticements need to be understood by state CIP practitioners who may need to leverage them in their relationships with the private sector.

One enticement that the NIPP suggests is that the government–private-sector relationship support a clear national interest by insuring that the entire spectrum of CIKR is protected, which—to the advantage of all partners—also reduces the risk to individual sectors and assets. Other enticements to private-sector partnership with government as envisioned in the NIPP are that private industry is afforded

- "Participation in both policy development and risk analysis";
- "Greater information sharing regarding specific threats and hazards";
- "Targeted application of limited resources to the highest risk issues, to include federal grant funding";
- "Joint R&D and modeling, simulation, and analysis programs"; and
- "Access and input into cross-sector interdependency analysis."[66]

Presumably, each of those NIPP-proposed benefits is of sufficient value to attract the private-sector partners targeted by this government protection effort. A state government CIP practitioner should be aware of whether his private-sector partners value these enticements; he should exploit the areas that the private sector values and find a mechanism to cajole their interest where they otherwise do not find value.

The NIPP suggests that the private sector has many contributions to make to support the national CIKR protection effort, including their ability to

- Perform risk assessments;
- Implement security practices to reduce vulnerabilities;
- Understand sector dependencies and cross sector interdependencies;
- Assist federal, state, and local governments in their CIKR inventories;

[66] *NIPP*, 2009, 11.

- Coordinate emergency response with federal, state, and local governments;
- Abide by industry best practices for security and share security best practices, implement "resilient, robust and/or redundant operational systems";
- Promote CIKR protection education and training programs and/or share security risk and threat information.[67]

Of these actions, facilitating private-sector security information sharing with respect to identifying threat, risk, and mitigation actions is a priority effort for the federal government. Other federal priorities for the private sector include providing a CIKR sector's or system's operational information to government protection practitioners and assisting government's CIKR practitioners with asset data collection and protection efforts. The NIPP encourages the private sector to voluntarily assist the government in its CIKR protection efforts. The NIPP presumes private-sector cooperation. In order to gain the private sector's cooperation, it is important for government CIP practitioners to appreciate the reasons that the private sector may be reluctant to engage in tasks as outlined in the NIPP.

A significant roadblock to the private sector's willingness to share threat, risk, and vulnerability information with government lies in sharing proprietary information that, if leaked, presumably could compromise a company's marketplace advantage over its competitors. In 2002, Congress acknowledged and remedied this very real information control concern of private industry when it passed the Protected Critical Infrastructure Information (PCII) legislation. PCII restricts access to critical infrastructure information and protects that information from release via Freedom of Information Act (FOIA) requests as well as state government "sunshine laws." The legislation requires the collector of PCII to practice rigorous information protection protocols. Critical infrastructure information (CII) that is collected by federal employees or entities

[67] *NIPP*, 2009, 24.

collecting the information on behalf of the federal government that meets the legislated criteria of CII will be afforded the PCII protections. PCII-qualified information cannot be used for regulatory purposes.[68]

Another important aspect of the public-private information sharing issue revolves around government actually sharing threat information or intelligence with private industry. The crux of the threat information sharing issue is evident in comments penned by General Robert Marsh, who wrote, "A specific challenge that still eludes us is defining an effective relationship between public and private sectors. Effective sharing of threat, vulnerability, and incident information—essential to the protection of our infrastructures—has advanced little in spite of the rhetoric, commissions, councils, and strategies that dot the critical infrastructure landscape. Effective frameworks for working together, schemas for information sharing, and incentive mechanisms, here and abroad, still have not emerged."[69] Given that General Marsh's comments are accurate and that a perception exists that little progress has been achieved in the national CIP effort, why waste time getting involved in government's stagnant effort?

This author's professional experiences surrounding the issue of sharing threat information with the private sector led to the opinion that the issue is related more to the private sector's perception that government does not trust it to share intelligence than to the government's resistance to share information. While assigned to the State Fusion Center at Logan International Airport, many private sector representatives that I interacted with believed that the threat information provided to them could not be all the available relevant threat information. In my experience the private sector perceived that federal and state government were not sharing threat information with them due to a lack of trust. State government shared the threat information it had that it believed was relevant for the private sector to implement security operations against those threats. In general, the lack of specific information shared is due to the lack of credible, specific information relevant to CIKR protection.

---

[68] PCII information provided is based upon the author's Department of Homeland Security–sponsored PCII training required to conduct CIKR assessments and to use the Automated Critical Asset Management System. More in-depth information can be found at www.dhs.gov/xlibrary/assets/CII_Act.pdf.

[69] Marsh, "Foreword," xv.

A well-developed public-private partner relationship would go a long way for government and the private sector to learn about the others' information needs and expectations. With respect to threat information sharing, the private sector perceives that the government mistrusts it because it is not receiving specific intelligence about threats to CIKR. The state CIP practitioner must engage the private sector in regular work groups and seminars to develop the trust needed to assuage private-sector concerns about being left out of the threat information sharing loop, to gain an understanding of the private sector's information needs, and to develop effective emergency response plans integrating the private sector. We will look at the private sector's concerns about partnering with government in the next section.

2. Private-Sector Concerns

To be effective partners in the CIP protection partnership with the private sector, government CIP practitioners should understand the management and business operational reality that influences private-sector security decisions. To that end we will examine an interesting daily reality of the private sector that affects its decision making—the constant pressure to increase competitiveness through operational efficiency and the vulnerabilities stemming from that reality.

a. Vulnerabilities of Efficiency

Technology and automation are often used to trim operational costs. Unnecessary costs are eliminated by leveraging outside networks such as the Internet for communication. Reliance on the Internet as the backbone of communication may expose a corporation to risk beyond its ability to mitigate. The constant pressure to increase competitiveness by reducing costs may result in a corporate decision not to further invest in security measures that would protect against a threat assessed as a low probability. Additionally, as noted by Auerswald, et al., "Competitive pressures do not allow firms to make large investments aimed at reducing vulnerability to disasters that are highly unlikely and nearly impossible to predict."[70] Stephen Flynn aptly postulates that, "the

[70] Auerswald, et al., "Where Private Efficiency Meets," 5.

reluctance to invest in security stems from managers' need to make infrastructure open to as many users as possible, efficient as possible, reliable as possible and low cost as possible to use. Because the conventional view of security is that it raises costs, undermines efficiency, is at odds with assuring reliability and constrains access, there has been a clear disincentive for the private sector to make it a priority."[71] However, the public or private-sector CIKR asset owner's ability to insure delivery of goods and services is directly contingent upon securing the assets that facilitate delivery of service. From the perspective of the asset owner, properly securing those assets is a good business practice commensurate with exercising due diligence. An asset owner's failure to insure the protection of assets from reasonable threat might then make the asset owner liable through the legal principle of vicarious liability.[72]

b. Endogenous or Exogenous Vulnerabilities

Auerswald's writing team describes security vulnerabilities as either "endogenous," borne of human error, or "exogenous," resulting purely from an act of nature where human action did not factor into the event. Unfortunately, in our interconnected, modern, and efficient society we are highly vulnerable to the endogenous events that may spread across networks.

The location and type of the next act of terrorism, an endogenous event, is for the most part unpredictable. In the security world the ability to gauge the degree of risk to which a CIKR asset is vulnerable is integral to the security investment decision. That investment decision becomes more challenging when a terrorist group practices what Auerswald's team refers to as "adaptive predation."[73] Adaptive predation is described as the adversarial tactic of adapting one's modus operandi (MO) to exploit gaps in existing security protocols that were enacted to mitigate the adversaries' current MO.

---

[71] Flynn, "Brittle Superpower," 30.

[72] During the years I worked as a state police detective, prosecutors in both the Office of the Middlesex District Attorney and the Office of the Attorney General, where I was assigned, discussed applying the principle of vicarious liability to hold organizations responsible for their employees' acts or failure to act.

[73] Auerswald, et al., "Where Private Efficiency Meets," 7.

That tactic makes it extremely difficult to invest in a security protocol that potentially becomes operationally irrelevant soon after implementation. In addition to terrorist threats, we willl now review other threats that CIKR managers must consider.

Auerswald identifies three types of low probability, high-consequence events that must be considered by industry managers: natural disasters like earthquakes or hurricanes, "'technogenic' disasters resulting from bad systems design, inappropriate regulatory frameworks, and political managerial failure"; and terrorist attacks.[74] Auerswald identifies four broad categories of action that industry can take to insure delivery of services by compensating for the low-probability, high-consequence events. Those categories are "managing organizations, securing networks, creating markets and building trust."[75] Each of the broad categories of action will be reviewed to establish mitigation actions available to the private sector. Of the four categories of action recommended for the private sector, managing organizations, creating markets, and building trust seem to be areas that state government would promote. Securing networks at the CIKR sector level potentially exceeds the ability of state and local jurisdictions to lend meaningful support. However, securing networks is an area where state and local CIP practitioners should be conversant, and it will be briefly touched upon later in this chapter.

B. MANAGING FOR RELIABILITY

Interestingly, with respect to managing organizations, Auerswald uses the FAA as an example of how to operate a critical service under severe pressures, facing a range of threats, including the low-probability, high-consequence event, while continuously delivering effective, reliable service. The premise is that because the FAA rate of failure is so low FAA management practices should be considered as a model for private-industry CIKR owners and operators to emulate in order to insure the reliable delivery of

[74] Auerswald, et al., "Where Private Efficiency Meets," 10.

[75] Ibid., 12.

service. That is, effective management matters. Effective management is an investment that all CIKR partners can make that will realize benefits during daily operations as well as during a crisis.

1. Reliability Through Effective Management

The operative concept in the following analysis of a successful management practice is reliability. Setting the goal of delivering reliable service as the objective of critical infrastructure strategy is a departure from the government's current framing of the issue. As noted by Todd La Porte with respect to critical infrastructure protection, "Since the issue surfaced in the early 1990s, public and business leaders have directed the public's attention toward *critical infrastructures*, rather than, say, *essential services*; toward *protection* of those infrastructures, rather than *assurance* of the services these infrastructures deliver." [76] Assurance of service incorporates actions that include physical and operational security measures—technology investments to streamline business processes—but more importantly it incorporates management practices of high functioning organizations, such as the FAA, with a near-flawless track record of delivering reliable service.

The current infrastructure protection paradigm for law enforcement and security professionals focuses CIKR protection efforts toward actions such as physical security measures, distributing assets, or protecting critical nodes to mitigate vulnerabilities. As described by LaPorte, emergency managers view the solution to the CIKR protection effort from the perspective of avoiding disaster by building assets in areas outside of hazard zones, responding to emergencies by dispatching first responders, and recovering from disasters by cleaning up damaged areas, rebuilding damaged assets, and restoring services.[77] Yet, another alternative to avoiding significant and costly disruptions is through strong, effective management.

[76] La Porte, "Managing," 71.

[77] Ibid.

In an article, “Managing for the Unexpected,” La Porte contends that the emergency manager’s solutions are important contributions. Unfortunately, those solutions to critical infrastructure assurance miss the real value of effectively managing infrastructure systems to assure reliable service throughout a disaster. However, La Porte acknowledges that the management practices that insure reliable service may impinge on a company’s financial bottom line. Those practices incorporate redundancy, intensive and repeated operator training, and frequent equipment testing and replacement. Insuring that these practices are implemented consistently throughout and across all sectors is challenging.[78] An important note in this effort is that in our open and free society CIKR spread over a vast geographic area cannot be guaranteed to be reliable all the time. CIKR is exposed to operational risks daily. Private sector management of those risks will be addressed in the next section.

2. Managing Risk

The process of calculating and managing risk is integral to the CIKR protection mission and will be addressed more thoroughly in the next chapter. Now we will briefly review the private sector’s perspective of managing risk. In order to consistently and reliably deliver service under modern marketplace pressures, it is necessary for companies to effectively balance risk. Competitive pressures often drive a risk management calculus that results in finding the operational point where there is sufficient security to protect an asset while facilitating a smooth, efficient operation. An extreme example of an unbalanced, yet secure operation might be an airline implementing a security program that restricts passengers from bringing luggage onto the aircraft in order to guarantee that a terrorist does not secret a bomb in the luggage. Those extreme measures would likely drive customers away and lead to the company’s going out of business.

A CIKR owner would utilize comparative risk analysis to decide what degree of risk he is willing to assume in comparison to the imposition of recommended security

[78] La Porte, “Managing,” 73.

practices in order to minimize the risk on his operation.[79] During that process risk managers would also consider the concept of countervailing risk. Countervailing risk addresses whether the steps implemented to mitigate one threat in fact create a secondary risk that is worse than the original threat it was created to avoid.[80] These risk analysis steps are important to calculate accurately in order for a company to develop a business model that allows competition in the marketplace while assuring reliable service.

The following section will review some suggestions from Robert Frosch and Todd LaPorte for managing CIKR toward the reliable delivery of service.

a. Redundancy

One suggestion, when designing operating systems or processes, is to build in redundancy where design engineers most expect critical components to fail. Redundant systems may add to the cost of an operating system, but in the right places they can geometrically improve the reliability of a system. Robert Frosch addresses the value of creating redundancy by adding more humans to oversee an operation. His idea is that added sets of experienced eyes overseeing a process will more likely detect a problem in the system and therefore remedy a problem more quickly than a company with fewer managers to detect and solve problems. Frosch acknowledges that adding additional managers must be factored within reason to avoid creating countervailing risk in the form of "coordination tax," where too many additional management layers creates delays in communicating directives to resolve a situation. Frosch addresses this consideration by pointing out that other "organizational means," such as creating trust in the workplace, can mitigate coordination tax. Conceptually, a high level of trust across all echelons of employees who share information about the process and effectively communicate identified problems would bring about solutions and eliminate the need to add an additional layer of management.[81]

---

[79] Frosch, "Notes Toward a Theory," 78.

[80] Ibid., 81.

[81] Ibid., 89–90.

b. The Value of Reliability

The company that reliably delivers its goods or services is valued. Private-sector managers strive to achieve value for the company through reliability. However, according to Frosch, it is necessary to find a balance point between being reliable and being functional. Frosch argues that "in the attempt to create a high reliability organization, the greatest problem seems to be achieving the balance between organizational discipline (necessary for its existence and reliability) and the open, informal structure needed for a functioning team. The countervailing risk to the high reliability team is that bureaucratic niceties will become a kind of self-defeating solution to problems. Formal discipline can destroy exactly those properties of the team that make it function."[82]

Todd R. La Porte identified characteristics of the highly reliable organization, as in Figure 2.

State CIP practitioners need to understand the reality of operating CIKR in the private sector and to appreciate the risk management practices that assure the delivery of service. The next section will review the topic of network security and the risk that private sector networks create for CIKR.

[82] Frosch, "Notes Toward a Theory," 95.

Internal processes:

1. Strong sense of mission and operational goals, commitment to highly reliable operations, both in production and safety
2. Reliability enhancing operations
   - Extraordinary technical competence
   - Sustained, highly technical performance
   - Structural flexibility and redundancy
   - Collegial, de-centralized authority patterns in the face of intense, high tempo operational demands
   - Flexible decision making processes involving operating teams
   - Processes enabling continual search for improvement
   - Processes that reward the discovery and reporting error, even one's own
3. Organizational culture of reliability, including norms that stress the equal value of reliable production and operational safety

External processes:

1. External watching elements
   - Strong super-ordinate institutional visibility in parent organization
   - Strong presence of stakeholding groups
   - Mechanisms for "boundary spanning" between the units and the "watchers"
   - Venues for credible operational information on a timely basis

Figure 2. Characteristics of the Highly Reliable Organization (from LaPorte, "Challenges")

C. NETWORK SECURITY

With respect to securing networks, the underlying premise is that most CIKR sectors are only as secure as the weakest link in the networks that connect them. The nature of the interconnected CIKR world means that an asset that has practiced security due diligence within a given sector may be at risk to damage due to the weak security of another asset within the same network. This same propagation of risk or cascading failure within a networked CIKR sector due to the poor security practices of one entity also applies across interconnected CIKR sectors where one underprotected asset can infect other CIKR sectors. This network vulnerability is addressed in depth by Dr. Ted Lewis in his book *Critical Infrastructure Protection in Homeland Security*. The dependencies and interdependencies within and across networked critical infrastructure sectors are complex. Dr Lewis advises that the most effective manner to secure a network is to

identify the critical nodes linking the network and invest resources toward securing those nodes before investing in each individual asset in the network.[83]

1. What Is the Threat?

When discussing network security the average individual probably thinks of the Internet, computers, and cyber security. In his chapter "A Cyber Threat to National Security?" Sean Gorman questions whether the cyber threat is as significant as is often described in the media. Gorman cites *Washington Monthly* columnist Joshua Greene, who claims, "There is no such thing as cyber terrorism—no instance of anyone ever having been killed by a terrorist (or anyone else) using a computer. Nor is there compelling evidence that Al Qaeda or any other terrorist organization has resorted to computers for any sort of serious destructive activity."[84] What, then, explains the national concern from this threat?

Much of the furor in the media over a terrorist threat against critical infrastructure utilizing cyber systems may be overblown. Prognosticators exist with opposing views as to whether the threat is significant or not. An interesting study undertaken by the Navy War College to simulate a cyber attack against CIKR revealed that "a group of hackers couldn't single handedly bring down the United States' national data infrastructure, but a terrorist team would be able to do significant localized damage to U.S. systems." Gorman noted that the researchers predicted that an attack targeting nationwide infrastructure would require "$200 million in funding, country level intelligence, and five years of preparation."[85] That study certainly establishes some parameters for discussing the nature and extent of the cyber threat. Quite likely, terrorist groups would not present a significant national cyber security threat unless they were backed by a nation-state providing the group with intelligence and significant funding. Nevertheless, the study indicates that our CIKR could be at risk from a nation-state that could exploit our cyber networks to attack our national infrastructure.

---

[83] Lewis, *Critical Infrastructure Protection*, 22.

[84] Gorman, "Cyber Threat?" 239.

[85] Ibid., 241.

Of greater national concern is the fact that numerous nation-states are developing cyber warfare capabilities. Currently, the strength and abilities of the United States military are unparalleled. No other military can match our military's strength. Other nations must use asymmetric means to undermine our nation's military advantage and often look to exploit cyber vulnerabilities to degrade our military capabilities. Cyber attacks initiated by nation-states against the United States may target our industries in order to disrupt those systems and undermine our national power or to conduct electronic espionage to steal proprietary information. In a recent example, the Chinese government was accused by Google of conducting cyber attacks against computers and servers within its network.[86] There is mounting evidence that the threat of cyber attack is growing, but what is vulnerable in the cyber network?

2. Cyber Network Vulnerability?

Cyber systems are composed of physical infrastructure like fiber optic cables, juncture boxes, servers, hubs, and computers. Each of the components is vulnerable to physical damage as a means to disrupt the network it is part of. Poorly designed software, the second component of a cyber network, creates another risk to the network. According to Gorman, there has not been enough research to indicate whether vulnerabilities in physical components or vulnerabilities in software place cyber networks more at risk to damage. Cyber attacks initiated through the exploitation of software vulnerabilities receive a good degree of publicity, but none of those attacks has resulted in a catastrophe. "While cases of major catastrophes from cyber attacks have not yet been documented, the tools, motivations, abilities and potentials have been documented."[87]

Gorman sets the table, explaining, "In no other critical infrastructure sector are vulnerabilities more publicly seen than in cyber systems, which include the logical and physical network of computers, servers, fiber optic cables, and other components that constitute the nation's information infrastructure. Worms, viruses, and denial of service attacks happen daily, and the largest and most devastating are covered in the media." He

[86] Markoff et al., "In Digital Combat."

[87] Gorman, "Cyber Threat?" 247.

later states, “The question with cyber security is not whether there are vulnerabilities, but whether there is a threat that warrants federal involvement, or whether it is simply a business issue that should be left to the market.”[88] As noted earlier, market strategies in other CIKR sectors aimed at streamlining operational costs to enhance competitiveness create vulnerabilities. So, too, the existence of vulnerabilities in cyber networks is attributed to software and systems designers who take shortcuts in their quality-control procedures in order to develop a product more inexpensively.

3. What Can State Government and the Private Sector Do?

Although these cyber warfare issues are real concerns, the detection and response to nation-state–directed cyber attacks within the United States are within the realm of the federal government and not that of state government or the private sector. An area of cyber security where state government can assist the national effort is to become knowledgeable and conversant in cyber security issues. State government must implement industry best practices, enter into partnerships with local industry focused on facilitating network security, and encourage local industry to implement best practices as well. The goal of encouraging all to maintain the best-practices standard for cyber security relates to network theory, where managing the risk of damage to an entire sector requires strengthening all assets in that sector. The underlying premise is that the risk facing one entity in a network or supply chain may be mitigated by the actions of all the entities within that network. Making the case within a network that encourages all the participants to invest similarly in security may prove challenging. However, influencing a number of entities to invest appropriately for security may be enough to initiate a change of action that influences the remaining entities to invest appropriately.

Ultimately, it may take financial incentive to industry to implement responsible cyber security practices. The state government should engage its federal government partners to provide incentive for private industry. One mechanism to generate incentive for the private sector to comply with enhanced CIKR security is through insurance. Gregory Jaksec discusses the government utilization of insurance regulations to impose

[88] Gorman, “Cyber Threat?” 240.

CIKR security standards on the private sector in his thesis, *Public-Private-Partnering in Critical Infrastructure Protection*.[89] Imposing additional insurance regulations may not be necessary to achieve private-sector compliance. Appealing to private sector altruism may be more successful in achieving enhanced CIKR security standards. Convincing the first few asset owners to comply may be what is needed to get all to comply. The benefits and limitations of the insurance option will be analyzed next.

D. THE INSURANCE OPTION

An emerging topic related to critical infrastructure assurance is the creation of a new market to assure infrastructure reliability. There is a growing market within the insurance industry for terrorism insurance. Within the realm of critical infrastructure protection, insurance is viewed as a tool to promote infrastructure assurance. Private industry may view the insurance proposition like this: insurers are acknowledged experts on risk analysis and risk management; and insurers are members of the private sector who can evaluate an industry's secrets without raising industry's concern of government intervention and regulation. An insurance company underwriting a CIKR asset may require the asset owner to invest in security measures that reduce both the infrastructure asset owner's risk and the insurer's risk. However, the notion that the process of insuring an asset may prompt the asset owner to invest in security measures to reduce its risk exposure and conversely reduce the insurance premium may prove false.[90] A company that is insured for loss may calculate that it does not need to invest in security to mitigate or deter a threat event because it is insured against losses incurred from that threat event. Insurance may prove not to be the entire solution to the private sector's ensuring reliable delivery of service, but it is a component of the overall solution.

The insurance remedy as a mechanism to infrastructure assurance is worthy of note. Consider, for example, the need to return life to normal as quickly as possible in the aftermath of a catastrophe or large-scale attack. Well-insured asset owners could be compensated quickly, allowing them to quickly repair their operations and return to

[89] Jaksec, *Public-Private-Partnering*, 18.

[90] Auerswald, et al., "Protecting Critical Infrastructure."

delivering goods and services. A lack of insurance coverage could delay the return of services due to a lack of funding to rebuild. Funding a rebuilding effort can be a huge undertaking. For example, the costs to recover from 9/11, Hurricane Katrina, or more recently the BP oil spill cleanup costs and financial compensation to those unable to work in the aftermath of the spill have been astronomical.[91] Neither the government nor industry alone could fund the recovery operations. Insurance companies helped to spread the cost of recovery. In many catastrophes the insurance industry is an important partner in the recovery operation. Businesses with the proper insurance coverage were better postured financially to more quickly return to operation.

There are challenges to the insurance solution. For example, in order for insurance companies to calculate the insurance rate or premium they must know the degree of risk to which an asset is vulnerable. In actuarial tables historical data is utilized to calculate the likelihood of a catastrophic event and the degree of risk to which an asset is exposed. As to the likelihood of a terrorist attack targeting a given asset, calculating the type of attack that will occur and calculating the resulting degree of damage is difficult. "One of the central issues at stake in the financing of catastrophic risks is to determine appropriate insurance mechanisms with specific premiums for events with relatively low frequency and with the potential to inflict massive disruption and/or destruction."[92]

The degree of uncertainty inherent in calculating the risk exposure that an asset faces from terrorism and in setting commensurate premiums to spread the risk may be a deterrent to insurance companies. Conversely, the cost of premiums imposed by the insurer on high-risk assets may exceed the willingness of the clients to pay. The insurance company approach to high-risk assets may entail requiring industry to mitigate vulnerabilities by implementing prudent security measures to lower its risk exposure as a precondition of coverage under a policy.[93] Potentially, the insurance-induced security measures may be less stringent than a company would consider taking to protect against

[91] According to Erwann O. Michel-Kerjan, the insurance costs for the 9/11 attacks are calculated to be $35 billion, and the insurance costs for Hurricane Katrina are calculated to be $45 billion. The insurance costs for the Gulf Coast, BP oil spill are ongoing. Michel-Kerjan, "Insurance," 286.

[92] Ibid., 284.

[93] Auerswald, et al., "Protecting Critical Infrastructure."

loss if it were not insured. Of course, in some cases insurance-imposed security measures could be more stringent than those of a company that elected not to implement any security measures because of the drain it would place on the bottom line.

There is no established minimum standard for security measures designed to mitigate vulnerabilities to critical infrastructure. Although there are many varieties of physical security measures to deter, detect, or mitigate a terrorist threat, the government has not established the minimum standard to be adopted by the private sector. Complicating the issue of setting security standards is the reality that many business owners do not believe that they are at risk of being the target of a terrorist attack. Without the perception of a higher level of threat that one's business will be directly impacted by a terrorist attack, what is the incentive to invest in insurance? Further complicating this issue and undermining the insurer's ability to make terrorism insurance policies attractive by offering credit for security measures implemented is the fact that "no research to date has defined causal relationships linking specific mitigation measures with quantifiable reductions in terrorism loss, there is no technical basis for an insurance pricing credit."[94] The lack of appropriate metrics to objectively measure the return on a security investment will be analyzed later in this thesis.

Certainly government has a role to encourage the insurance industry to participate in underwriting insurance policies for CIKR owners. Government involvement in the aftermath of a catastrophe can affect future efforts of insurers. If the government compensates all of the affected entities for their loss, there is no incentive for entities to insure themselves in advance of an event. Also, government actions in advance of terrorist action may impact whether that event actually takes place or whether it achieves the impact as planned. Those actions can reduce the amount of risk that an insurance company assumes when underwriting a CIKR asset. Effective government-led recovery actions in the aftermath of a catastrophe can also significantly reduce the financial losses incurred and by extension limit the amount of claims that insurers pay to customers.

[94] MacDonald, "Terrorism, Insurance," 327.

The symbiotic relationship between government action and insurers' actions with respect to pre- and post-catastrophe actions must be cultivated in order to manage the impact of catastrophes and to establish a greater CIKR resilience. The foundation for that government/private-sector relationship could be built on trust.

E. THE ISSUE OF TRUST

Building mutual trust among the government, the private-sector partners in CIP, and the public may be the key to successful critical infrastructure protection. As evidenced in the 2009 NIPP, the federal government understands that it must build trust with the private sector in order to achieve its goals in CIKR protection. The private sector must ensure the trust of its customers as well as the government, whom they will rely upon to assist them to avoid or recover from a disaster. Establishing and maintaining trust will be a continuous and difficult journey. As Branscomb and Michel-Kerjan acknowledge, "The habits and cultures and the legal, political, and financial power among a complex mosaic of stakeholders differ in many ways. This leads us to an essential element of all enduring and successful partnerships: The necessity for building trust between the parties."[95]

1. Trust Built on Information Sharing

Information sharing could be an exploitable mechanism to develop a mutually trusting relationship between government and the private sector. As addressed earlier in this thesis, information sharing is an important component of an effective CIKR protection strategy. There is a potential stumbling block to government's sharing of intelligence with the private sector. Private industry desires government intelligence information to develop more relevant and effective security measures. Governments releasing that information to the private sector could jeopardize or compromise intelligence information gathering operations and sources.[96]

---

[95] Branscomb and Michel-Kerjan, "Public-Private Collaboration," 395.

[96] Ibid., 398.

The challenges to effective information sharing transcend all levels of the national protection effort among federal, state, and local governments and the private sector. There are many different and apparently competing interests that can obscure and confound the information sharing process. Clearly, in our global economy, with interconnected CIKR crossing national borders, mutual trust between not only industry partners but nations as well has become a necessity. It will take strong leadership to develop trust among all the partners. It will take even stronger and committed leadership to maintain those trusted relationships.

2. Valuing and Protecting Proprietary Information

We addressed the PCII protections afforded to private-sector CIKR proprietary data collected on behalf of the federal government. Those PCII protections do not provide information protection, though, for proprietary information to be shared among industry competitors. Consider the following potential problems of sharing proprietary information within industry:

- Information about a company's security vulnerabilities may be of interest to other companies networked in the industry purely for calculating and managing their own potential risk;
- One company's proprietary information, if disclosed to a competitor, could eliminate the first company's competitive advantage;
- Certain elements of data, if released to competitors, could compromise privacy clauses between industry and its customers.

How, then, does one convince owners and operators of private-sector CIKR to share their security vulnerabilities with one of their competitors?

A proposed solution by Branscomb and Michel-Kerjan to overcome private industry's reticence to share information with its competitors entails creating "trusted information sharing platforms." The platforms would be populated with proprietary information collected by a third party to the CIKR asset owners. The third party would aggregate the data, remove privacy information, and then allow industry partners access

to the aggregated data to evaluate important security trends.[97] Federal and state government can play a role in encouraging industry leaders to develop information sharing relationships with their competitors and government. Government can be the third party to share information pertaining to prevention, mitigation, and recovery plans, and government could provide threat and risk information based upon vetted intelligence. It should not be a surprise to realize that the information gathering and processing capabilities of some private corporations may exceed or parallel those of government agencies. In that regard some industry partners may have information or intelligence of interest to government. Nonetheless, the degree of information sharing required to attain the level of situational awareness necessary to effectively secure CIKR sectors does not currently exist. Developing a culture of information sharing could perpetuate the trusting relationships necessary to maintaining that culture. Government at all levels must be involved in developing the culture and maintaining the relationships between the government and the private sector. Those government actions will be addressed more in the next chapter.

[97] Branscomb and Michel-Kerjan, "Public-Private Collaboration," 396.

THIS PAGE INTENTIONALLY LEFT BLANK

V. THE CRITICAL INFRASTRUCTURE PROTECTION ROLES OF STATE GOVERNMENT: TACTICAL AND STRATEGIC

As addressed earlier in this thesis, the 2009 NIPP recommends a series of general actions that state governments can take to support the national infrastructure protection effort. The 2009 NIPP also recommends the Risk Management Framework as a structure for the states to follow in order to coordinate their CIP efforts with federal and private-sector partners. The NIPP does not prescribe specific steps to be taken by the states to best accomplish the recommended actions. The absence of specific guidance suggests that the federal government lacks the knowledge and experience to offer more definitive guidance on how to effectively carry out its recommendations. Alternatively, the cover letter for the *Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal and Territorial Levels,* a federal government–developed companion document to the NIPP, may explain the federal government's failure to mandate specific steps. The cover letter explains that the guide was not intended to be "prescriptive"; rather, it was intended to "suggest various strategies and approaches"[98]s and leave it to the state or local government's discretion as to whether or which suggestions to incorporate into their state CIP plan. That same sentiment may be a common influence on other federal guidance.

In 2003, the Council of State Governments released the *State Official's Guide to Critical Infrastructure Protection*, with broadly identified objectives for a state protection program. The guide recommended that states focus on coordination, communication, and information sharing; develop partnerships with the federal government, other states, and the private sector; conduct scenario-based exercises; and conduct vulnerability and risk assessments of identified critical assets.[99] The guide establishes that national preparedness and response is also an important element of the overall protection effort. The guide also lacked definitive guidance. The lack of specific guidance creates a gap where states must educate themselves about CIKR protection and determine how they

[98] DHS, "Guide to Critical Infrastructure," cover letter.

[99] Hopkins, *State Official's Guide*, 54.

can best achieve NIPP-stated goals. Absent prescriptive and definitive guidance, it is incumbent upon a state to provide the specific protection roles to be executed within its jurisdiction.

In that light the following chapter will review the possible implementation steps for state government to fulfill its CIP mission. There is an abundance of potential tactical and strategic critical infrastructure protection roles that a state government may undertake. In this chapter those roles will be culled from the 2009 NIPP, the DHS-developed *Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal and Territorial Levels*, and the state infrastructure protection strategies of the states of Arizona, Washington, and Virginia. Each of the five documents was evaluated and cross-referenced to determine consensus and divergence regarding the roles for a state government in CIP. Based on that analysis and my professional experience working in infrastructure protection, recommendations will be offered regarding actions that merit inclusion in the CIKR protection strategy of Massachusetts.

In the context of the national infrastructure protection effort, it is important for a state government to understand its strategic role in order to maximize its contribution and insure a return on its investment of resources. In an undertaking the size and complexity of infrastructure protection, unity and synergy of effort is important at every level. As with each of the entities involved in CIKR protection (federal, state, and private sector), state governments must coordinate their efforts with the federal government and private industry to avoid duplication of effort and to focus their resources in the most advantageous area.

This chapter will utilize the six stages of the Risk Management Framework suggested in the 2009 NIPP as a format to analyze the state roles recommended in the NIPP and to evaluate the recommendations. The NIPP recommends both tactical and strategic steps. The chapter will identify which of the suggested roles are tactical in nature and recommend how a state can develop and coordinate the capacity to achieve the tactical objectives. The chapter will further address the strategic roles with the objective of recommending how the state of Massachusetts can achieve a strategic CIP impact on behalf of its residents and the nation.

A. THE TACTICAL ROLES OF STATE GOVERNMENT

The NIPP suggests that CIP efforts can include the following wide range of activities:

- Improving security protocols;
- Hardening facilities;
- Building resiliency and redundancy;
- Incorporating hazard resistance into facility design;
- Initiating active or passive countermeasures;
- Installing security systems;
- Leveraging self-healing technologies;
- Promoting workforce surety programs;
- Implementing cyber security measures;
- Conducting training exercises; and
- Planning for business continuity.[100]

From the perspective of state government, the majority of these actions are tactical and generally appropriate to address the security vulnerabilities of individual assets or groups of assets. If applied effectively, the actions reduce the vulnerability of specific assets to a postulated threat; they are appropriate recommendations to public or private CIKR asset owners. However, although many of these steps are relatively simple to implement, they may not always be appropriate or represent the best solution to vulnerability. For example, some infrastructure by its nature may not be targeted by terrorists. In such a case hardening facilities, installing security systems, or initiating active or passive countermeasures may not be necessary.

The CIP practitioner requires a level of knowledge, skill, and experience in CIKR protection in order to make recommendations that are relevant and that effectively

[100] *National Infrastructure Protection Plan*, 2009, 7.

mitigate the postulated threat. A poor-quality effort from a state vulnerability assessment team that recommends physical-security solutions where there is no threat only provides bad data, undermines the credibility of their findings and recommendations, and may lead to wasted security resources and diminished rapport among the CIKR partners. Understanding the realistic threat and the risk to infrastructure sectors and their assets is critically important to conducting relevant vulnerability assessments. In the aftermath of 9/11, without a clear understanding of the threat to our nation's infrastructure, inexperienced CIP practitioners caused unnecessary investments to be made in physical security, wasting financial and emotional capital for public and private-sector infrastructure operators.

For the most part the actions listed above, where incorrectly applied and implemented, do not achieve a strategic effect. They do not create a result where the effort expended to execute the action achieves an effect many times greater than the effort expended. The goal of the state CIP practitioner is to apply an appropriate blend of tactical actions in areas that are identified through intelligence analysis as being likely targets of attack or other damage and that through risk analysis present significant vulnerabilities warranting the investment of resources to achieve a strategic security posture.

The strategic application of resources is easier said than done. Although a challenge, it can be achieved by dedicated, experienced, and educated CIP professionals. The leader of a state's CIP program needs to perform like the Leonard Bernstein of critical infrastructure protection. To expand the metaphor, the CIP leader must understand CIKR and perform like the brilliant maestro of an orchestra, who synchronizes the professional musicians, in this case CIP partners from both the public and private sector. The score for the CIKR symphony would be the state infrastructure protection strategy.

Virginia's Critical Infrastructure Protection and Resiliency Strategic Plan supports this maestro-like metaphor when it directs that its Office of Commonwealth Preparedness (OCP) "will lead in the development of Vulnerability Assessment Teams, whose members will be subject matter experts drawn from State, Local and Private Sector

entities. The Vulnerability Assessment Teams will support all Sector Specific Agencies in developing their Sector Specific Plans."[101] Virginia has identified an appropriately high-level state entity, the OCP, to "conduct" its CIP effort with well-qualified subject matter experts at its direction. That portion of its strategic plan recognizes the need to oversee the state CIP effort from a prominent position in state government resourced with experts. Making that statement a reality will achieve a strategic impact for the state. The following will address more strategic roles for a state.

B. THE STRATEGIC ROLE OF STATE GOVERNMENT

Prior to the 2009 NIPP, much of federal infrastructure protection guidance addressed "protecting" infrastructure. The term "protection" was widely used in previous federal guidance and remained a nebulous term. The established federal narrative of "protecting" critical infrastructure evoked the perception that CIKR sectors or assets must be secured from the threat of terrorist attack and remain safely operational 100 percent of the time. Assets that are 100 percent secure or safe is an unrealistic goal in an open and free society. A distorted perspective of the actual risk that CIKR faced warranted a national reframing of the CIKR protection narrative away from a predominantly focus on terrorism to a broader understanding of managing the greatest risk. As government infrastructure protection practitioners learned more about the challenges of "protecting" single CIKR assets, they also better appreciated the need to focus more efforts on managing risk across a sector. The 2009 NIPP evolved to focus more on risk than previous federal strategies had, explaining that the protection effort "includes actions to mitigate the overall risk to CIKR assets, systems, networks, functions, or their interconnecting links resulting from exposure, injury, destruction, incapacitation, or exploitation."[102]

---

[101] *Commonwealth of Virginia, Critical Infrastructure Protection*, 8.

[102] *National Infrastructure Protection Plan*, 2009, 7.

The 2009 NIPP incorporated the Risk Management Framework as the foundation for the most recent federal CIP effort. The Risk Management Framework is composed of six core functions that DHS recommends that a state critical infrastructure protection program fulfill. The six steps are identified as:

- Set goals and objectives;
- Identify assets, systems, and networks;
- Assess risk;
- Prioritize CIKR across sectors;
- Implement protective programs and resiliency strategies; and
- Measure the effectiveness of the risk mitigation efforts.[103]

Figure 3 depicts the six steps of the federal risk management cycle, as well as the three broad threat sources (physical, cyber, and human) from which to evaluate the risk to CIKR.

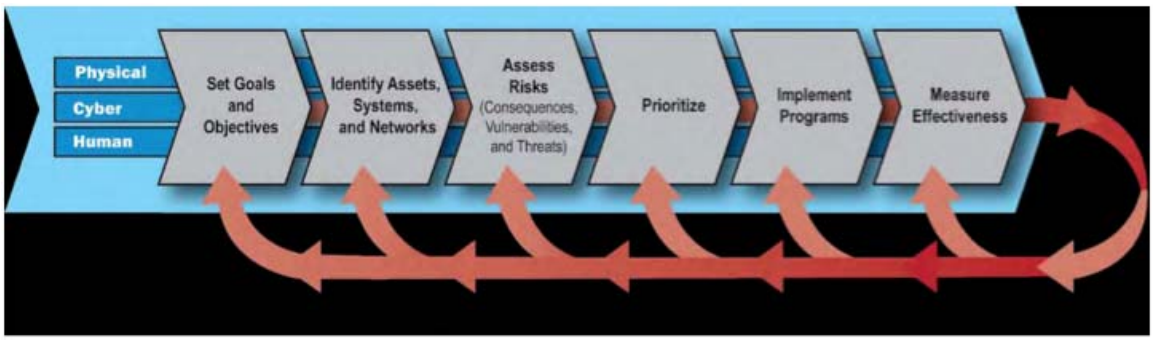

Figure 3. Risk Management Framework (from NIPP, 2009)

We will now review the six steps of the Risk Management Framework as they are addressed in the NIPP and review the three state CIP strategies to ascertain how they intend to fulfill those six steps.

[103] *National Infrastructure Protection Plan*, 2009, 163.

1. Set Goals and Objectives

In a strategy the goals and objectives define the intent of the plan and provide focus for the effort. The NIPP explains that "goals and objectives define specific outcomes; conditions, end points, or performance targets that collectively constitute an effective risk management posture."[104] It further establishes the overarching goal of the national CIP effort: "Nationally the overall goal of CIKR-related risk management is an enhanced state of protection and resilience achieved through the implementation of focused risk-reduction strategies within and across sectors and levels of government."[105] Each state has been left to determine how it will focus its resources to achieve CIKR protection through risk reduction. The goals evident in each of the three state critical infrastructure plans analyzed strike me as too broad and as having been written for political rhetoric more than to define the parameters of the plan and to give appropriate direction.

For example, the Arizona plan, which was written in 2006, before the current NIPP was released, does not seem to be synchronized with current federal CIKR protection goals. The Arizona plan establishes three goals: 1) to ensure that first responders have access to personal protective equipment; 2) to improve communication systems to allow first responders to communicate during emergencies; and 3) to bolster security in the state.[106] The stated goals in the context of the plan do not seem to be relevant to coordinating the state effort with the federal CIKR protection effort. The goals seem intended to bolster the intent of justifying federal money to achieve a state desire to fund the purchase of emergency management equipment. The third goal to bolster state security is so broad as to be meaningless as a mechanism to provide direction for the CIP effort.

Alternatively, the overarching goal of Virginia's critical infrastructure protection plan is "to ensure a Virginia whose communities, businesses and government are safe,

---

[104] *National Infrastructure Protection Plan*, 2009.

[105] Ibid.

[106] State of Arizona, *Infrastructure Protection Plan*, 12.

secure and prepared." That is a broad goal that provides context to the effort. This broad goal is then more keenly focused through seven supporting goals that synchronize that plan with the NIPP:

- Identification and protection of CIKR deemed most critical;
- Timely warning for CIKR facing a specific, imminent threat;
- Enabling a collaborative environment with government and the private sector;
- Ensuring that sufficient funding is available to mitigate CIKR risks;
- Integrating the Virginia plan with the NIPP;
- Understanding, protecting, and sharing information about terrorist threats and other hazards; and
- Building security partnerships for long term risk management.[107]

Each of the supporting goals orient the state's CIP partners to the objectives they should strive to achieve.

Interestingly, the Washington State Infrastructure Protection Plan (WIPP) does not directly state the plan's goals. Rather, it explains the purpose of goals in general and references the Washington Statewide Homeland Security Strategy as the source for the WIPP's goals. The WIPP establishes that its public and private-sector protection partners are expected to adopt goals whose intent is "to maintain and sustain critical and essential services that support a normal way of life for the citizens of Washington State."[108] The Washington Statewide Homeland Security Strategy identifies as the state's CIKR goal to "Develop and Sustain an Infrastructure Protection Program."[109] Its homeland security strategy states that the Washington Military Department, Emergency Management Division will lead the statewide CIP effort; it lists a series of supporting objectives to help achieve the statewide objective. The stated objective of the strategy generally

[107] Commonwealth of Virginia, *Critical Infrastructure Protection*, 3.

[108] *Washington Infrastructure Protection Plan*, 5.

[109] Ibid., 23.

supports the goals addressed in the NIPP. The decision to assign the responsibility of overseeing the state CIP program to the state military department has value in that the military members have likely had experience protecting infrastructure, conducting vulnerability assessments, and organizing and executing complex strategies from their traditional military mission. Massachusetts could be well served to mirror the Virginia plan's goals and objectives and to mandate the involvement of its National Guard resources.

An integral component of the national CIKR protection effort is conducting asset inventory of the CIKR sectors in each state. The asset inventory is an important tactical-level task for state governments to undertake that produces a strategic effect. The next step in the NIPP risk management cycle that we will evaluate is the process of identifying CIKR assets within the jurisdiction.

2. Identify Assets, Systems, and Networks

Before prioritizing what is and is not important, a state must identify the infrastructure and supporting assets in its jurisdiction. The DHS intends to leverage the state and local government relationships with private-sector CIKR owners so that those entities will perform a significant portion of the national CIKR inventory data collection. A web-based tool, Constellation/Automated Critical Asset Management System (C/ACAMS), was created to facilitate state, local, and private-sector entities' input of CIKR data into the federal database.[110] The actual inventory of infrastructure in a state is a tactical function from which the aggregate of the collected data should create strategic understanding. Once the inventory is compiled, the stratification of critical from noncritical begins.

With an amorphous national CIKR definition, the list of assets that potentially qualify as critical infrastructure in any given state grows. Inventorying assets and identifying those assets that qualify as critical based on current federal guidance and practice is a daunting challenge. Establishing criteria for stratifying the importance or

[110] *Washington Infrastructure Protection Plan*, 31.

criticality of infrastructure and its commensurate assets is a necessary component of infrastructure protection. States should enjoin the federal government to reframe the national CIKR narrative to help practitioners understand that all infrastructure is not "critical" and to establish a clear distinction between basic infrastructure and "critical" infrastructure. A state strategic plan needs to focus the predominate effort on ensuring the protection and functioning of "critical" infrastructure.

Unfortunately, in the national CIKR arena, the definition of "critical" is lacking. Dr. Bellavita makes an important point that "the initial difference between critical infrastructure and plain vanilla infrastructure seems to have quietly vanished."[111] Today almost everything related to infrastructure assumes some level of criticality. As noted in an issue of the Heritage Foundation's *Backgrounder*, the term "criticality" is overused. The article describes the following condition: "Policymakers, uncomfortable about acknowledging that not all attacks or accidents can be prevented, turn to criticality as a crutch—pouring more and more resources into all infrastructure instead of tailoring dollars to those that are truly critical. Essentially, there is an incentive to deem infrastructure critical because of the resources that become available from such a designation."[112]

Both points strike at a significant element, albeit an unnecessary one, that dramatically complicates an already complex issue. From my research it appears that the lack of understanding by many involved in infrastructure protection has fostered the expansion of the term "critical." The fact that federal grant dollars are tied to protecting infrastructure creates an incentive for politicians and CIP practitioners to term assets as critical in order to qualify for protection funds. It will take a very strong hand to end this misdirected effort and force CIP practitioners, public and private, to better understand and more accurately qualify what infrastructure is truly critical. That simple "criticality" discriminator will filter out the unimportant and enable states to focus diminished resources on the important. The *Backgrounder* article suggests that practitioners "disaggregate what is 'critical' (essential for sustaining and supporting Americans' daily

[111] Bellavita, "How Proverbs Damage," 2.

[112] McNeill and Weitz, "How to Fix," 4.

lives) from what is 'dangerous' (e.g., chemical facilities) but not necessarily critical."[113] To establish the most functional list of true CIKR, political influence must be eliminated.

A review of the recent evolution of the definition of "critical infrastructure" as it has evolved across federal directives, from the release of the Patriot Act in 2001, the Homeland Security Act in 2002, HSDP-7 in 2003, and other homeland security strategies, including the most current definition in the 2009 NIPP, may enlighten the issue. The 2009 NIPP standard CIKR definition is "systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any federal, state, regional or local jurisdiction."[114] The federal definition of "critical" infrastructure is significantly broad to avoid creating a definition that unintentionally excludes an asset. That is understandable when considering that the federal definition will be applied across this great and expansive nation. Unfortunately, the NIPP's broad definition of critical infrastructure or very close derivatives of it are regularly repeated in state homeland security strategies. The broad definition has the effect of disbursing the CIP practitioner's focus to all infrastructure assets. Despite the lack of a clear federal definition of "critical," each state is free to create a more definitive description of what constitutes "critical" infrastructure within that state, and it should do so.

Without a refined definition of "critical," there is an ever-expanding inventory of CIKR maintained in the federal infrastructure data warehouse (IDW), with contributions from the DHS, Sector Specific Agencies (SSA), state governments, and the private-sector owners of CIKR. In order to stratify the inventory data, the DHS created the National CIKR Prioritization Program, which qualifies CIKR that has national significance as either Tier 1 or Tier 2 assets. The criteria for both Tier 1 and 2 assets are described as those that, "if destroyed or disrupted, could cause some combination of significant casualties, major economic losses, or widespread and long-term disruptions to national

[113] McNeill and Weitz, "How to Fix," 4.

[114] *National Infrastructure Protection Plan*, 2009, 109.

well-being and governance capacity."[115] The federal government, through the DHS and the SSAs, maintains primary responsibility for maintaining the inventory of Tier 1 and Tier 2 assets.

However, Tier 1 and 2 assets fall within the jurisdiction of state governments, who have a responsibility to protect those assets. Protection of the Tier 1 and Tier 2 CIKR falls under the federal Buffer Zone Protection Program (BZPP). The BZPP is the responsibility of the DHS Office of Infrastructure Protection, PSAs, and FEMA. In each state after Tier 1 and Tier 2 assets are identified a state should begin to stratify and prioritize the remaining critical assets in its jurisdiction by their importance to the state. Insuring that those assets deliver their commensurate services will be the responsibility of a given state and its private-sector partners. In order to prioritize the attention given to infrastructure in a state, whether through physical-security investment, enhanced operational or security processes or enhanced resiliency, the risk to a given asset or CIKR sector must be assessed. Correctly assessing risk to a sector and the assets within that sector will have strategic effects by influencing decisions about how to best insure that a sector delivers its service. Risk assessment is another contentious issue in CIP and will be analyzed next.

3. Assess Risk

Risk assessment methodology has been a contentious issue in homeland security since 2001. In the period of time since 2001, the DHS has introduced a number of risk formulas to be utilized by states to calculate risk to infrastructure. Application of those risk formulas created contention centered on the outcome of risk assessments conducted by the states. The outcome of those state risk assessments determined the amount of federal homeland security grant dollars received by that state. Politics seems to have influenced the risk methodology selected by the federal government. An analysis conducted by the Congressional Research Service (CRS) regarding the risk methodology formulas selected by the federal government illuminates the history of risk assessment problems and discusses the strength of the current methodology.

[115] *National Infrastructure Protection Plan*, 2009, 41.

The evolution of the federal risk assessment methodologies affords some insight for the CIP practitioner to appreciate that there are different methodologies and that a given methodology may affect the outcome of the analysis. Immediately after September 11, 2001, through FY 2003, the federal formula for calculating risk was as simple as "risk = population (R=P)."[116] This formula essentially means that the population of a region drives the degree of risk to that region. This was an extremely rudimentary formula that did not facilitate stratification of CIKR based upon risk. Considering the simplicity of the formula, it seemed to be more oriented toward spreading federal dollars to pacify politicians than toward effectively identifying which critical infrastructure was most at risk and allocating protection dollars for protection efforts to mitigate the risk. The following year, in 2004 to 2005, the DHS risk calculation formula was altered to factor population density (PD), threat (T), and critical infrastructure (CI) where risk R=T+CI+PD.

During the reign of Michael Chertoff as secretary of the DHS, in 2006, the next change to the federal risk methodology coincided with the secretary's directive that risk management would underscore the department's calculus for the dispersal of grant funds. Under Chertoff the DHS risk formula was R=T*V*C. "This new approach to allocating the remaining funds required an assessment of risk using a formula that considers the threat to a target/area, multiplied by vulnerability (V) of the target/area, multiplied by consequence (C) of an attack on that target/area."[117] Multiplication of the factors of risk gave each factor a weighted value, allowing for stratification of risk among CIKR assets within a sector and also across CIKR sectors.

To compare the levels of risk to CIKR assets and sectors across the spectrum of CIKR sectors, it is necessary to establish a common baseline by utilizing a single formula for all calculations of risk. Unfortunately, the realistic application of risk theory across all postulated threats does not lend itself to a clean analysis process. There is still a great

[116] Masse, O'Neil, and Rollins, "Risk Assessment Methodology," 5.

[117] Ibid., 6.

degree of subjectivity introduced into the calculation with respect to an asset's vulnerability to a threat. The DHS therefore decided to assign a value of one for vulnerability to eliminate it as a variable.

The 2009 NIPP has established the latest risk formula to be R=f(C,V,T), where risk is considered to be a function of consequence, vulnerability, and threat. The DHS considers it to be important that its partner in the national CIP effort understand risk to be influenced by the nature and magnitude of the threat, the vulnerabilities to that postulated threat, and the consequences that could result.[118]

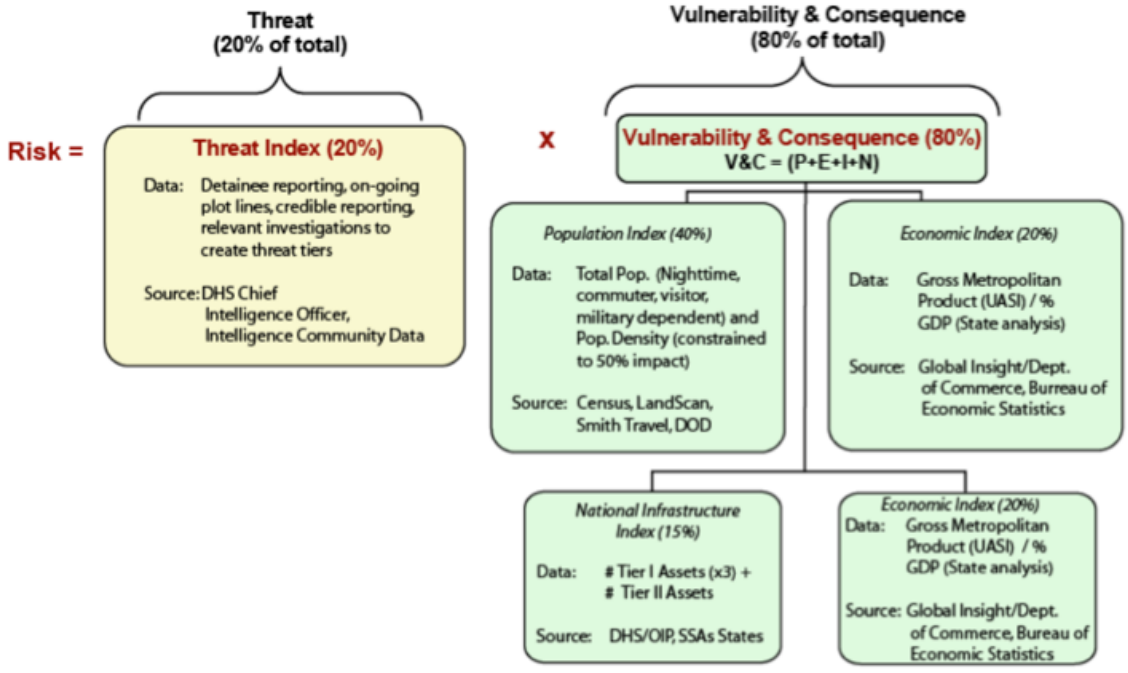

Figure 4. DHS FY 2007 Risk Formula (from Masse, O'Neil, and Rollins, "Risk Assessment Methodology, 8)

A study conducted by the National Research Council, available in the National Academies, stated that the "Committee finds that current Department of Homeland Security risk formula of Risk=f(T,V,C) is a philosophically suitable framework for

[118] Masse, O'Neil, and Rollins, "Risk Assessment Methodology," 32.

breaking risk into its component elements."[119] The premise of the analysis was essentially that the formula works conceptually to calculate risk from natural and man-made hazards, but it questioned the formula's ability to calculate risk in the "terrorism domain."[120] The DHS established a requirement that its adopted risk analysis formula meet four objectives: being documented, reproducible, defensible, and complete. The study found that the DHS's historical application of the formula did not meet the four required objectives.[121] That determination certainly brings into question the validity of the risk assessments conducted by DHS and its agents to date.

There are many challenges to managing the risk analysis component of the CIKR protection mission. The study in the National Academies Press questions the DHS's capacity to consistently produce accurate and effective risk analysis due to the limitation of available, experienced, and qualified risk analysis personnel to work on behalf of the DHS. This is an important factor for states that will need to rely on the risk analysis capacity of the DHS to support their own needs. The education level and depth of experience required for an analyst to develop a qualified opinion of the state of risk within a given sector makes it unlikely that every state could maintain a team of individuals dedicated to risk analysis. State CIP team members will require formal training in risk analysis in order to apply the appropriate risk modeling tools with credibility.

The state of Arizona's CIP strategy does not specify the risk formula used, but it does recognize risk as a factor of consequence, vulnerability, and threat. The strategy discusses the development of a statewide risk assessment. To provide a context for understanding risk to CIKR, Arizona elected to address consequence analysis in four categories:

- Health impact—Effect on human life and physical well-being;
- Economic impact—Direct and indirect effects on the economy;

[119] National Academies Press, "Review," 52.

[120] Ibid.

[121] Ibid., 53.

- Psychological impact—Effect on the public's morale and confidence in national economic and political institutions; and

- Governance impact—Effect on the government's ability to maintain order, deliver minimum essential services, ensure the public's health and safety, and carry out national security related missions.[122]

As discussed earlier, insurance companies analyze risk utilizing historical data to establish the likelihood of an event's occurrence or recurrence. Through historical data they are able to calculate the degree of risk of an event's happening and to calculate the potential loss from a particular threat. With respect to current critical infrastructure protection doctrine, risk must be calculated for the threat presented from Mother Nature's wrath, man-made accidents, and now the threat of terrorism. The terrorist threat is difficult to determine, and without an extensive terrorism actuarial table, it is difficult to predict the degree of risk from terrorism. Without precise intelligence it is difficult to predict the likelihood of a specific type of terrorist event occurring at a specific location in order to calculate the consequence of that event to that asset or infrastructure sector.

Intelligence collection, analysis, and dissemination in the context of information sharing is necessary to facilitate the ability of CIKR partners to measure the threat picture for their jurisdiction. Creating and maintaining effective information sharing processes has been a work in progress for fusion centers. Appropriate information sharing remains an integral component of accurately calculating threat. The NIPP information sharing solution lies in the development of trusting relationships, partnerships, and coordination across federal, state, and local government, as well as private-sector CIKR owners. Figure 5 is a visual model of the NIPP information sharing concept.

Calculating a sector's or region's level of risk is an important first step toward prioritizing an appropriate vulnerability mitigation plan for a specific asset or whole sector. The following section will address how a state should prioritize CIKR and its response to calculated risk.

[122] State of Arizona, *Infrastructure Protection Plan,* 13–14.

Figure 5. NIPP Networked Information Sharing Approach (from NIPP, 2009, 60)

4. Prioritize Critical Infrastructure Across Sectors

The complexity and expanse of CIKR in an interdependent society challenges the resources available to secure the full infrastructure spectrum. Presumably, not every sector is equally important to the functioning of a modern society, and not all assets within a CIKR sector are equally important within that sector. From the perspective of a given jurisdiction responsible for securing infrastructure, economy of forces becomes critical. Maximizing the available resources to assure that infrastructure delivers its service to maintain a functioning society requires an accurate selection of the most critical assets within each system and across CIKR sectors. Prioritizing which infrastructure sector is more important to society over another and which asset within a sector is more important can become contentious when opinions and priorities are not in sync.

The breadth and magnitude of the CIKR sectors can be an overwhelming concern to those tasked to protect them. The fact that there are sector-specific agencies at the federal level with assigned responsibilities to coordinate securing each of the CIKR sectors does little to diminish the concern of the state practitioners tasked at the ground level to secure them. The federal sector-specific agencies can be a resource to state government to help navigate the spectrum of CIKR when prioritizing its effort to secure CIKR sectors or assets. In order to facilitate the state-level management of CIP, the commonwealth of Virginia established a state-level sector-specific council (SSC), responsible to the Office of Commonwealth Preparedness (OCP); it dictated that each of those agencies insure that the risk management framework is followed.[123] Tasking sector-specific agencies at the state level achieves a strategic effect by parceling responsibility across multiple agencies, thereby freeing the OCP to coordinate and guide the overall CIP effort. Each Virginia SSC is able to focus more intensely on the issues concerning infrastructure in its sector and to understand how to prioritize that sector's needs.

Federal guidance within the 2009 NIPP recommends that, in order to prioritize CIKR, a jurisdiction should compile and compare risk assessments to gain situational understanding of each of its sector's individual risk. After aggregating the assessment, it should be able to establish priorities based on risk and create "protection, resilience or business continuity initiatives that provide the greatest return on investment for the mitigation of risk."[124] However, ensuring a corporate regard for securing CIKR among all parties with a vested interest in CIKR is a challenge. Gaining mutual understanding of an asset's importance or criticality and then agreeing to the stratification of an asset against other critical assets may be contentious. Appreciating which components or assets truly merit protection and then understanding the degree of protection that an asset warrants is an essential component of the overall state protection effort. An important

[123] Commonwealth of Virginia, *Critical Infrastructure Protection*, 11.

[124] *NIPP*, 2009, 28.

consideration in this effort is a tenet of Sun Tzu: to defend (protect) everything is to defend (protect) nothing.[125] How, then, is the final prioritization of CIKR accomplished?

The NIPP guidance suggests that CIKR prioritization includes determining which "regions, sectors, or other aggregation of CIKR assets, systems or networks have the highest risk from relevant incidents or events." Those that face the greatest potential loss will receive the greatest attention in developing risk management solutions. The second step is to determine, of those assets prioritized to receive risk management assistance, which will likely realize the greatest risk mitigation for the investment. In this regard much of the NIPP guidance remains general and ambiguous, subject to interpretation and adherence to prioritization seemingly at a given state's will.

The state of Arizona establishes that its state government "will identify, prioritize and coordinate protection of critical infrastructure and key resource" but does not identify how prioritization will be calculated.[126] Virginia also accepts responsibility through its Office of Commonwealth Preparedness (OCP) to prioritize the protection of CIKR by leveraging its state sector-specific councils to conduct the prioritization and protective efforts.[127] Similarly, Washington State utilizes the Infrastructure Protection Sub Committee (IPSC) to prioritize "CIKR having statewide or broader impact." [128] Additionally, the state of Washington provides a general explanation of how that prioritization will be achieved by factoring notional outcomes to terrorism, natural disaster, and emergency scenarios.

a. The Important Versus the Unimportant

The basis for the contention created during efforts to prioritize CIKR within a given jurisdiction can be summed up in the expression "One man's trash is another man's treasure." Invariably, there will be varying degrees of consensus as to which CIKR asset is figuratively considered to be trash as opposed to treasure.

---

[125] Sun-Tzu, *Art of War*, 192.

[126] State of Arizona, *Infrastructure Protection Plan*, 7.

[127] Commonwealth of Virginia, *Critical Infrastructure Protection*, 11.

[128] *Washington Infrastructure Protection Plan*, 6–7.

With respect to public policy, when prioritizing an asset based on its perceived criticality, the relevance of a CIKR asset may become defined somewhat in the context of "where one sits often dictates where one stands" on the issue. In that light there are generally different opinions about what is important from the different perspectives of federal, state, and local jurisdictions. Politics, whether federal, state or local, can certainly be a factor that will influence which assets make the criticality list and where those assets rank in importance for protection dollars. Presumably, the higher degree of criticality that a sector or an asset rates; the greater the resources that society expends to secure it.

Absent politics infrastructure prioritization differences of opinion may exist simply because of an individual's vocation in life or location in life. For example, a small-town mayor may believe that her town hall is a critical asset to the community's well-being and that it should receive protection dollars. However, that town hall has absolutely no relevance to the overall nation's well-being and it is therefore unimportant from a federal perspective. Now, of course, this example is absurd and simplifies the issue to make a point that there may be dramatic differences of opinion about what is critical. Also, priorities will change over time as society's needs change. Once again, a clear definition of what is critical infrastructure, including examples, will ease the CIP process.

b. National, Regional, State and Local Perspective

Prioritizing CIKR assets may be a contentious process even within a local community. By extension the stratification process of CIKR at the national level must be even more so. The national-level stratification is the concern of the federal government, but that national process will undoubtedly affect many state and local communities where different CIKR assets are located. As an example, consider that a critical node of the communication sector is located in a community that is unaware of that asset's function and critical importance. That single building could link numerous components of that sector or be a single point of failure for a region of the country. The loss of that node could lead to an instant loss of the network. Under certain threat conditions a local

jurisdiction could be responsible for securing that asset. With respect to this notional communication asset, the local and state jurisdiction where that asset is located should have a say in how that asset is stratified and regarded at the national level. They should be involved in the asset's vulnerability assessment and in the discussion of how to prioritize that asset.

On the other hand, it is possible that a CIKR asset is located in a local jurisdiction where the locals are aware of the asset's importance to an infrastructure sector or that it is a critical node that links multiple sectors together but the federal or state government is unaware. Coordination and effective communication across all entities with a potential interest in an asset's welfare is necessary to ensure that all levels of government are aware of an asset's importance and that they establish who will protect that asset. The previous discussion underscores the importance of effective public and private partnerships.

5. Implement Programs

In the area of homeland security, it is frequently said that 85 percent of this country's infrastructure is owned by the private sector. Accepting the accuracy of this statement raises a significant issue for federal and state governments about how to ensure that the CIKR that is owned and controlled by the private sector remains viable to deliver the service or goods that this country requires to sustain our way of life. What mechanism can the government use to ensure that the private owner of CIKR assets takes the reasonable measures to protect critical assets from damage? Should the government establish regulations and enforce standards of protection for an infrastructure sector? Or is the solution to allow the private-sector owners the freedom to establish an industry standard for security and hope that market competition will create pressure on the owners to effectively secure their assets in order to remain competitive within that sector? This issue was debated by the Marsh Commission. The findings of the commission can be found woven throughout much of the federal strategy to protect infrastructure. As explained by General Robert Marsh regarding the commission's debate on these issues,

> As one would expect, there was lively debate regarding the many possible options. They ranged from government-centric solutions involving legislation and regulation prescribing mandatory remedial actions by industry and government, to the opposite extreme of voluntary actions prompted by political leaders' urgings through stressing patriotic duty and the national interest. After much deliberation we concluded that the private sector has a clear responsibility to protect itself from the lesser threats, such as individual hackers and criminals, and the government has the larger responsibility to protect the citizens from national security threats.[129]

A general understanding of the Marsh Commission's report and findings will greatly enhance the aptitude of any practitioner of critical infrastructure protection. Their findings, if accepted, will help determine the nature and focus of a state CIP program with respect to the roles played by government and the roles played by the private sector.

There is no one-size-fits-all solution to this problem. In his thesis Gregory M. Jaksec writes about the benefits of government regulation as a mechanism to ensure that infrastructure sectors meet operation standards. Jaksec refers to the federal regulations imposed by the Federal Energy Regulatory Commission (FERC) on the energy sector as an example of the government's involvement to ensure delivery services.[130] Of course, excessive government regulation of a sector could thwart its ability to remain competitive in the market place. To insure CIKR delivery of services, Jaksec proposes a blend of solutions to include public-private partnerships and government-supported incentive packages that include security standards, insurance underwriting, and tax incentives. [131]

We will consider next the private-sector and public-sector involvement in a state CIP program.

a. Private Sector

Federal strategies including the 2009 NIPP identify the need for government entities to include and rely upon the private sector in the CIKR assurance

---

[129] Auerswald, *Seeds of Disaster*, xiii.

[130] Jaksec, *Public-Private-Partnering*, 17.

[131] Ibid., 35.

efforts. The ongoing recovery efforts unfolding in the Gulf of Mexico today with respect to British Petroleum's handling of its runaway oil well spill and the allegations of unsafe oil rig operations leading to the spill bring into question the wisdom of relying wholly on private industry to manage any infrastructure sector owned by it. An article in *Business Week* lays out some of BP's history of safety transgressions surrounding oil production that may have been contributing factors in the Deepwater Horizon disaster. The article also identifies BP CEO Tony Hayward's admission that the company wasn't prepared to manage a spill of this magnitude. [132] If true, it would appear that BP could not be trusted to insure a safe and reliable delivery of petroleum products. But is the BP example isolated, a statistic aberration when factored across all the private industry-run infrastructures effectively operated over the years?

Consider another example: in Massachusetts a series of significant storms over the last few years has undermined public confidence in the state's major power company's ability to ensure the delivery of power or to quickly recover after a significant disruption. A significant ice storm, a rare Category 1–2 hurricane, and a mid-fall Nor'easter each caused limbs from trees and whole trees to break in much greater numbers. Regions lost power and for longer periods of time due to the extensive damage to power lines from the broken trees. What appears to be the underlying factor for the extensive loss of power and the prolonged outage was the power company's decision not to spend resources to better maintain vegetation-clear areas around the power lines.[133] In contrast, towns that received electricity from municipal power companies had less extensive loss of power and recovered from the loss more quickly than the privately owned "big" power companies. Why? The municipal power companies had invested time and resources to better maintain the areas around their power lines.[134] A government requirement to better maintain the power line rights of way may diminish the extent of damage from the effects of Mother Nature. However, government regulation of all CIKR

[132] Barrett and Blum, "Oil Spill."

[133] "Keller at Large: How to Fix Routine Power Outage Issues," *CBS Boston*, October 31, 2011. Retrieved November 3, 2011, from http://boston.cbslocal.com/2011/10/31/keller-large-how-to-fix-routine-power-outage-issues/.

[134] Pfeiffer and Jolicoeur, "Local Power Utilities."

sectors would create bureaucratic nightmares for the government to manage and would risk undermining the private sector's inherent capacity for flexible adaptation and improvement.

From the perspective of a state CIP program, the debate regarding whether infrastructure should be owned and managed by private industry is beyond its concern. Based upon my experience in the critical infrastructure protection program in Massachusetts, the state lacks the capacity to operate and manage each of the infrastructure sectors' industries. Private industry has the experience, knowledge, and resources to more effectively manage CIKR. To ensure the delivery of services, the reasonable alternative is for state government to establish a partnership with the private sector to effectively secure infrastructure.

Developing a relationship of trust with the private sector infrastructure owners in your jurisdiction is strategically important. Creating partnerships with the private sector CIKR owners in a state's jurisdiction is recommended in the 2009 NIPP and reiterated in numerous federal and state homeland security strategies, Congressional research, and academic research. Interestingly, the state of Alabama passed a law to ensure that cooperation and coordination among state, county, and local governments with private-sector CIKR owners is achieved.[135] The private-industry owner of infrastructure needs to be regarded as an ally in the protection effort and relied upon to help the government practitioner understand the operation and vulnerabilities of the wide range of infrastructure sectors.

b. Public Sector

For the sake of clarification, infrastructure sectors that are predominantly controlled and operated by the public sector are:

- Water supply and waste water treatment facilities;
- Highways and roads;

[135] Hopkins, *State Official's Guide*, 48.

- Public transportation, including rail service and airports managed by government agencies or government controlled authorities;
- Emergency services inclusive of police, fire, and emergency management; and
- Certain municipal electric power companies sprinkled throughout the country that generate power to support their region.

Responsibility to protect those sectors rests entirely on state and local government. Those sectors at a minimum must be at the fore of state and local efforts to ensure the continued delivery of services and goods. Vulnerability assessments should be conducted to inventory the important assets and nodes supporting public transportation, water supply and waste water treatment, and municipal power systems. Of those sectors that are publicly operated we will look more closely at the aviation industry in order to highlight the state government's role in that operation. For the majority of publicly owned U.S. airports, state government oversees management of the airport facilities and must provide security and law enforcement for the airport.

Independent of other threats, the aviation industry is identified in open-source reports as a principal and enduring target for al' Qaeda–influenced terrorists. Consider the challenge of insuring the viability of the U.S. aviation industry with direct links to most countries around the globe. The Transportation Security Administration (TSA) has the overall responsibility to insure the security of our aviation industry. In the air transportation realm, the TSA enforces security directives that mandate security requirements for the airport operator and for air carriers. Transportation security officers of the TSA are tasked to establish a layer of security at airports to screen passengers and cargo transported on the airplanes; the privately owned air carrier implements TSA-required security procedures; and state or local government implements security programs to support TSA directives. The aviation industry is a good example of the value of a public-private partnership ensuring the viability of an infrastructure sector. Although those partnerships are not formally named, at public airports the safe and successful operation of the airport is one measure of an effective partnership.

The next challenge for state government in its CIP journey is to measure the effectiveness of its program. This next section will review the guidance from the NIPP and the three state CIP strategies.

6. Measure Effectiveness

The 2009 NIPP states, "The use of performance metrics is a critical step in the NIPP risk management process to enable DHS and the SSAs to objectively and quantitatively assess improvements in CIKR protection and resiliency at the sector and national levels."[136] All the recommended metrics measure what is being done but not how effective the tasks accomplished actually were. It is nice to know what was done, but that does not necessarily indicate whether the intended effect was achieved or whether it was necessary at all.

The macro-level objective of DHS is to gauge whether the areas of CIKR deemed a priority for protection efforts are actually receiving the investment of attention and resources to mitigate any identified vulnerabilities. DHS is not objectively measuring whether the attention and investment in those prioritized sectors or assets are effectively securing those assets. The final measure should be that infrastructure continues to provide services whether the threat is from terrorism, Mother Nature, or poor engineering or process.

An appropriate metric may be, for example, that service was delivered uninterrupted for so many days or that when a service was interrupted, it was returned to normal operation in a certain period of time. Based on my military and law enforcement experience with security, the measure of a security program's effectiveness at preventing an attack is mostly subjective. The effectiveness of your program's security from a terrorist threat cannot be measured by the irrationality that if you are attacked, your program is ineffective, and if you are not attacked, it is effective. There is also another possible measure of an effective program: if terrorists were detected in their planning cycle and their intended attack was thwarted. A number of terrorist-intended attacks like

[136] *NIPP*, 2009, 46.

the Ft. Dix plot or the Times Square bombing were stopped by an observant citizen who reported suspicious activity. Law enforcement or security officers did not directly stop the attack, and we cannot directly measure their effectiveness on stopping the attack. However, it could be argued that public outreach and education through a "See something, say something" type of initiative was effective.

A review of the three state CIP plans with respect to measuring effectiveness revealed the following: The Arizona plan recognizes what metrics are generally intended to do but does not offer any information on the types of metrics to be used to measure the program's effectiveness. The Virginia plan acknowledges its requirement to measure its program's performance. The plan identifies the following four measures of success, generally stated as:

- Coordinated, risk-based CIKR plans and programs in place addressing known and potential threats;
- Flexible and adaptable structures and processes that adjust to lessons learned and best practices;
- Processes established to identify and address dependencies and interdependencies; and
- Access to intelligence, risk analysis, and real time incident reporting information sharing networks.[137]

The Washington plan provides the most detail on how the state intends to measure effectiveness. The Washington plan states, "Measuring effectiveness is a continuum influenced by technology, threat, resources and numerous other factors." The plan highlights resilience as the principle outcome if the program is effective. Washington identifies exercises as the most common tool to track effectiveness. The Washington plan identifies four mechanisms to measure effectiveness:

- Descriptive measures—used to understand sector resources and activities with examples like the number of facilities in a jurisdiction or the population within the area of an incident;

[137] Commonwealth of Virginia, *Critical Infrastructure Protection*, 4–5.

- Process (output) measures—tracking the progress of a task, reporting the output of a process with examples such as the number of protective programs implemented in a fiscal year, the level of investment in those programs, the number of detection systems installed in a facility, or the number of employees receiving training;

- Outcome measures—used to track progress toward a strategic goal by achieving results, rather than measuring the amount of activity. An example is measuring the reduction in risk for a given sector from one year to the next with a link to a specific protection process; and

- Ensuring an effective, efficient program over the long term—identify gaps, implement solutions, and reevaluate effectiveness utilizing four questions each with subquestions with four ratings (did not meet; nearly met; met; and exceeded) to select as an answer to each question.[138]

The Washington plan provides the most detail about measuring the effectiveness of the program. The measuring process forced the state to strongly critique the actions undertaken on behalf of the program.

As demonstrated in this chapter, the state government's role in critical infrastructure can be extensive. The following paragraph is taken in its entirety from the NIPP in order to make the point that a significant challenge is laid at the feet of state government:

> State and territorial governments shall develop and implement State or territory-wide CIKR protection programs that reflect the full range of NIPP-related activities. State and territorial programs should address all relevant aspects of CIKR protection, leverage support from homeland security assistance programs that apply across the homeland security mission area, and reflect priority activities in their strategies to ensure that resources are effectively allocated. Effective statewide and regional CIKR protection efforts should be integrated into the overarching homeland security program framework at the State or territorial level to ensure that prevention, protection, response, and recovery efforts are synchronized and mutually supportive. CIKR protection at the State or territory level must cut across all sectors present within the State or territory and support national, State, and local priorities. The program also should explicitly

[138] *Washington Infrastructure Protection Plan*, 10–11.

> address unique geographical issues, including transborder concerns, as well as interdependencies among sectors and jurisdictions within those geographical boundaries.[139]

The final chapter will offer recommendations from my research to incorporate into a state CIP program that will meet this challenge.

[139] *NIPP*, 2009, 21.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

This thesis serves to identify strategic roles that the state of Massachusetts should fulfill to effectively secure the delivery of infrastructure services within its jurisdiction. Review of federal critical infrastructure and key resource (CIKR) plans and strategies, other states' CIKR protection plans or strategies, academic research, and other writings on the topic provide sufficient rationale to propose a state government role in critical infrastructure protection (CIP). This chapter presents the conclusions garnered from this research to provide a framework for an effective infrastructure assurance program and a CIKR assurance strategy for the state of Massachusetts. A successful infrastructure assurance program would require the following steps to be implemented:

- Reframe the infrastructure protection narrative;
- Develop resilience in infrastructure and the public;
- Write a state CIKR protection strategy and develop an effective state CIP program;
- Select an experienced, knowledgeable, and influential individual to lead the CIP effort;
- Educate CIP practitioners, politicians, and the public;
- Develop appropriate public-private partnerships and sector-specific councils; and
- Create trust through transparent information sharing.

A. REFRAME THE NARRATIVE

1. Infrastructure Assurance

The research for this topic followed various information trails leading to the first conclusion that in order to effectively manage the infrastructure issue in this country, and more parochially in the state of Massachusetts, it is necessary to reframe the CIKR protection narrative. The nation's infrastructure narrative became focused on security of

infrastructure rather than assuring that infrastructure remain viable to deliver service. The first chapter of this thesis reviewed the recent history of infrastructure and the more recent history of the critical infrastructure protection debate. As evidenced, for example, in EO 13010[140] and the 2007 *National Strategy for Homeland Security*,[141] the infrastructure debate clearly became oriented toward a protection mission post–Desert Storm and focused even more acutely on critical infrastructure protection after the terrorist attacks on 9/11. The current narrative was further distorted since 9/11, when the spectrum of what qualifies as infrastructure that is "critical" began expanding within our current list of 18 CIKR sectors.

The critical infrastructure protection initiative may be losing focus due to mission creep. As pointed out by Dr. Bellavita and others, what qualifies as "critical" is convoluted. The stratification of CIKR across 18 sectors is not the problem, but qualifying each sector as a critical infrastructure sector creates the perception that everything contained in each of those sectors is critical and warrants protection. That perception of broad criticality contributes to complicating the infrastructure debate simply by unnecessarily increasing the volume of data related to the discussion. A more definitive description of "critical" would help to improve understanding of what infrastructure is critical and help to segregate "vanilla" or normal infrastructure from "critical" infrastructure.

The overarching infrastructure narrative should be oriented toward the assured delivery of services, rather than simply protecting CIKR. The goal of an infrastructure assurance strategy should be to provide targeted support to the infrastructure sectors, both from government and the private sector, so that quality services are delivered consistently and, if there is a disruption, that service is returned as quickly as practical. Services deemed critical would receive priority support toward assured delivery of service based upon a predefined ranking structure or process. To better focus the infrastructure assurance effort and rein in the critical infrastructure mission creep, it is necessary to better define what infrastructure is critical and what is normal.

---

[140] Executive Order 13010.

[141] *NIPP*, 2007.

To that end, within the state of Massachusetts infrastructure effort there should be two distinct categories of infrastructure: one "critical," the other "normal." Infrastructure deemed "critical" would qualify for regular maintenance support and prioritized protection effort, while the infrastructure deemed "normal" would qualify for the investment of resources oriented toward regular maintenance. During recovery operations in the aftermath of a significant man-made or natural disaster, infrastructure providing critical service would receive priority efforts to restore its associated service. Assurance of service requires the investment of capital and other resources in both types of infrastructure. Both types of infrastructure should be designed and operated with resilience in mind. Infrastructure resilience as a component of the state's CIP strategy will be addressed in section B of this chapter.

2. The New Critical

An element of the complexity of infrastructure protection derives from the limited understanding of what constitutes critical infrastructure or when infrastructure becomes critical. The definition of critical infrastructure in the 2009 NIPP remains broad and open to interpretation. A loose interpretation of what is critical will have the effect of expanding the list of infrastructure assets requiring support. Absent specific federal government definitions, a state government can establish a functioning definition of critical to that state's priority of effort assuring the delivery of service within the state. For example, a baseline definition of infrastructure that is critical might be an asset or network that, if damaged from a single, localized event, may either result in the immediate death of over 1,000 people, cause an immediate economic loss of more than $20 million, or result in the loss of service for greater than 14 days with a cumulative economic loss of over $100 million. The definition could be enhanced with examples of infrastructure that is critical, such as a certain capacity nuclear power plant, or a certain capacity hydroelectric dam, or a certain size chemical plant, or a node of a network such as electric, highway, pipeline, or cyber.

An ambiguous definition of critical infrastructure also provides unnecessary opportunity for the government CIP practitioner or politician, wittingly or unwittingly, to

proclaim that an asset is critical in order to qualify for federal funds. A more exact definition would prevent the misapplication of resources toward assets that would not realize the greatest return for that investment. State politicians, state government CIP practitioners, and their private-sector partners should engage the DHS and the federal government in a CIKR debate to force a discussion to qualify what is critical.

3. Understand the Threat

Ten years after 9/11, the infrastructure protection debate also needs to be reframed in the context of better understanding the threats from which we are trying to secure infrastructure. The nature of the threat should directly affect the steps taken to secure CIKR or provide infrastructure assurance. Infrastructure is susceptible to damage from man-made or natural threats. History has shown examples of infrastructure catastrophically affected by man-made or natural events. However, other than war or significant natural disasters, few of those historical events have had a national or regional catastrophic impact.

Avoiding catastrophe or responding to a catastrophe should be the primary government focus of the infrastructure assurance. In the context of threatening the stability of the United States, a country of over 300 million people spanning four time zones, a terrorist attack is not a catastrophic threat to the nation. Post 9/11, the nation focused on the postulated threat from terrorism. However, applying that threat to all infrastructure sectors and against each asset was not based in a realistic understanding of the threat.

Experienced state CIP practitioners need to engage the DHS and challenge federal guidance that does not support the ground truth in their jurisdiction. Challenge the homeland security paradigm, specifically in the area of risk assessment and threat assessment. Avoid the current urge to cast the threat of terrorism as the greatest threat to all 18 sectors of infrastructure. The aviation and rail components of the transportation sector have certainly been the target of many terrorist attacks throughout the world and deserve the added security attention they receive especially because of the potential second- and third-order effects realized after successful attacks against those targets.

Excluding the attacks of 9/11, the direct result of the majority of terror attacks does not achieve the level of strategic effect that warrants the expenditure of resources applied by the United States across the many infrastructure sectors.

a. Nation-State Threats?

An accurate threat picture, be it an act of man or an act of nature, is necessary to conduct worthwhile risk assessments that drive infrastructure assurance decisions. It is not clear that many CIKR protection strategies and security investments were based on a clear appreciation of the threat or were made by people who had the experience to make qualified security decisions. Some of the local security solutions undertaken in the years since 9/11 seemed to be more appropriate to defend against a sustained attack from an enemy nation. Maybe that was the threat understood by some local decision makers. An attack by a nation-state is not the type of threat that most state politicians or law enforcement consider. If that threat is a part of the federal risk calculus, state politicians and heads of local law enforcement need to understand the context of the threat to engender their commitment of state and local resources to assist in securing assets in their jurisdiction worthy of protection. However, protecting against an attack from an unfriendly nation is mostly the realm of the federal government such as the DoD, DOS, or DHS. Enemy nation threats, unless imminent, should not be the daily concern of state CIP practitioners. State National Guard assets should be part of the state CIP program and more intimately involved with the DoD to understand nation-state threats to their state if they exist and to coordinate appropriate responses at the state level. State government's focus should be focused on the more localized threats to infrastructure in its state, be it an act of man or an act of nature.

b. Threats of Nature or Threats of Man

At the state level, disruptions from nature are generally understood and predictable due to years of experience. Although extremes of nature are unpredictable, infrastructure assurance members need to consider the potential for a storm to strike with an intensity that greatly exceeds the norm. The ferocity and the subsequent compounded

effects from Hurricane Katrina in 2005 forced the federal government's infrastructure protection effort to refocus on the threats from natural disaster as well as the threat of terrorism. Actions to mitigate the effects of the median threats from nature are already mitigated in building codes and formalized emergency response procedures. A state infrastructure assurance program would rely on local building inspectors to ensure that infrastructure is built to code so as to withstand extreme weather. Emergency response to local weather disruptions is mostly formalized and the primary concern of state and local emergency managers. Infrastructure assurance practitioners need to be sure that true "critical" infrastructure is able to withstand or recover quickly from the most extreme weather.

On the other hand, man-made threats, especially from terrorism, are less understood and predictable. State CIP practitioners need to look to their state fusion center to gain a local understanding of the potential man-made threats in their region. In the event that the fusion center lacks the focus or capacity to provide valuable threat information, that information can be gained from the PSA assigned to that state or directly from HITRAC or the State, Local, Tribal and Territorial Government Coordinating Council (SLTTGCC). It is important to understand that threat and risk analysis are products of human analysts and inherently contain a degree of subjectivity.

State CIP practitioners should be informed and experienced in the spectrum of threats enough to challenge threat and risk assessments that do not comport with their understanding of the regional threat. The aggregate of localized threat should be contained in an annual risk assessment. A worthwhile risk assessment should provide a context to understand how a threat may make CIKR in the region vulnerable.

The federal solution of creating resilience to mitigate the effects of either man-made or natural threats is encouraged through the 2009 NIPP. Resilience is the best alternative to mitigate the spectrum of predictable and unpredictable threats facing infrastructure. Planned infrastructure resilience will be discussed next as a state government's response.

B. DEVELOP RESILIENCE IN INFRASTRUCTURE AND THE PUBLIC

Planning resilience to threats of man or nature can be achieved in a number of ways, as discussed in Chapter IV. Infrastructure resilience can be achieved through building redundant capacity, such as back-up facilities to replace damaged buildings, or through effective management processes and procedures that avoid disasters or efficiently recover from them. Building redundancy through back-up buildings or through engineering more robust systems can be prohibitively expensive. Depending on the function of a given facility and its criticality to the infrastructure system, redundant capacity may not be warranted. In those cases developing and implementing strong processes and procedures may be the most cost effective and wise practice to achieve resilience.

A hurricane, for example, has the potential to create regional devastation and indiscriminately disrupt assets located in its path. Yet within regions affected by hurricanes, there may be relatively very few infrastructure assets that will justify the advance investment in construction design engineering to help them withstand the force of a Class 4–5 hurricane. A region prone to hurricanes would better assure infrastructure services by preparing to effectively respond to and recover from the damage of a disaster. In the event of a hurricane, resilience built into the infrastructure systems in the form of redundant capacity, staff trained to respond and recover, partnerships trained and exercised to respond and recover, and a resilient population psychologically sound and ready to provide for themselves for a period of three to five days is necessary.

A state CIP program should be involved in identifying the threats to its region; identifying the critical infrastructure in its jurisdiction worthy of investment in redundant capacity through risk analysis, and helping to guide the development and implementation of effective management processes to avoid or respond to infrastructure disruptions. The state infrastructure assurance program should also help emergency managers and private-sector asset owners coordinate and exercise an effective response capability within their

jurisdiction. State government has a role to enhance the resilience of its population by their resolve and the capacity to support themselves for short periods during an emergency.

The state infrastructure assurance program can assist the federal government, state government, the private sector, and the public to develop the appropriate resiliency. There are many alternatives to develop a resiliency capacity in our society. An interesting example offered by Dr. Ted Lewis considers building "distributed generation" capacity into the power sector.[142] Essentially, this idea entails creating the capacity to generate electricity at the local level, for example, at a mall, a factory, or in a neighborhood using solar, wind, and fuel cell generators. The localized power generation creates redundancy in the system and nearly eliminates one of the sector's most vulnerable areas, the transmission and distribution of power.[143]

Alternative power generation solutions, like that offered by Dr. Lewis, are key to the long-term success of the state infrastructure assurance effort. The involvement of academics pushing the creative envelope for solutions to our nation's vexing infrastructure challenges is necessary to overcome government's potential for bureaucratic inertia. Next, we will discuss the framework for an effective infrastructure assurance strategy and an infrastructure assurance program to implement the strategy, which will include formalized partnerships between government, the private sector, and academia.

C. DEVELOP A STATE INFRASTRUCTURE ASSURANCE STRATEGY AND AN EFFECTIVE INFRASTRUCTURE ASSURANCE PROGRAM

1. Infrastructure Strategy

At this time, Massachusetts is without a state CIKR protection strategy. The state should develop a strategy oriented toward a new concept of overall infrastructure assurance, including a more focused entity to address CIKR protection of assets that

[142] Lewis, *Critical Infrastructure Protection*, 283.

[143] Ibid., 249.

warrant a greater level of support. To synergize with the federal CIKR effort, Massachusetts should develop a strategy that utilizes the NIPP risk management framework as a guideline similar to the strategies of Virginia and the state of Washington. State government roles should be articulated in a comprehensive infrastructure protection strategy that acknowledges the various efforts of public and private-sector partners and synchronizes those efforts toward insuring the delivery of infrastructure services in the jurisdiction. With respect to synchronizing partnerships, there are elements of the Virginia and Washington plans that bear inclusion in the Massachusetts strategy.

For example, Virginia established the Governor's Office of Commonwealth Preparedness (OCP). That state's strategy establishes that the OCP was mandated by the General Assembly and state code to oversee the combined federal, state, and local officials and the private sector and state sector-specific agencies. The fact that the OCP is state legislated provides OCP with the leverage to orchestrate the state's response. The strategic plan clearly establishes that the objective is to create "unity of results" and "unity of effort." The Virginia plan organizes the effort by distributing responsibility to state-level sector-specific agencies, a VA Plan Coordinating Council, and other boards, commissions, councils, partnerships, and the state military advisory council.[144] Importantly, the Virginia plan also establishes a program goal with supporting goals.

The state of Washington Infrastructure Protection Plan (WIPP) identifies its state's concern about damage cascading through its infrastructure networks and propagating loss. The WIPP mirrors the risk management framework and guidance provided in the federal NIPP. The WIPP broadly addresses all hazard threats as opposed to focusing primarily on the threat of terrorism. The WIPP does not delineate goals for its plan but declares that their goals are located in the Washington Statewide Homeland Security Strategic Plan. One of the two goals in that plan is Goal 4.1: Develop and Sustain an Infrastructure Protection Program. The goal is supported by a series of well-focused initiatives.[145] The Washington strategy, similar to the Virginia strategy, creates

[144] Commonwealth of Virginia, *Critical Infrastructure Protection*.

[145] *Washington Statewide Homeland Security Strategy*.

subcommittees, like the Committee on Homeland Security's Infrastructure Protection Subcommittee (IPSC), populated with representatives from the state-level sector-specific councils that represent public-private partnerships.[146]

The Washington plan describes how the state will calculate the consequence of a disaster, utilizing the categories for analysis (people, economy, environment, property) reflected in the acronym PEEP. Each category of PEEP has an assigned lead agency tasked to manage the consequence of an event affecting infrastructure within its scope of responsibility.[147] The WIPP includes a developed resiliency program that also bears emulation. Finally, as identified in Chapter V of this thesis, the WIPP has developed a series of questions, each with a commensurate series of subquestions to enable the state to measure the progress of its protection plan.[148] The questions allow the state to gauge those tasks accomplished toward the overall goal. Although the questions do not quantify the effectiveness of the efforts, they are a good starting point for the state of Massachusetts to incorporate into its strategy.

In addition to incorporating some of the highlights from the Virginia or Washington plans, Massachusetts should develop more detailed goals, define who is responsible to accomplish those goals, and legislate funding to sustain the initiative.

2. State Infrastructure Program

The state of Massachusetts should create a broad infrastructure assurance program that focuses on assuring infrastructure's consistent delivery of service. The program should be mandated in legislation much as the Office of Commonwealth Preparedness in Virginia. The infrastructure assurance (IA) program would maintain an inventory of the normal infrastructure as well as the "critical" infrastructure. Within the state infrastructure assurance program there should be a subgroup that focuses exclusively on the "critical" infrastructure in the state and on steps to insure that critical infrastructure is effectively secured from threats.

---

146 *Washington Infrastructure Protection Plan*, 4.

147 Ibid., 5.

148 Ibid., 10.

The infrastructure assurance program should be comprised of members representing multiple disciplines and multiple agencies from state and federal government and should include representatives from the private sector and academia. The private-sector representatives bring a wealth of experience in infrastructure assurance and understand the reality of market pressures with respect to corporate investments in infrastructure security. Academics bring fresh ideas, well-developed critical thinking skills, the willingness to challenge the status quo, and finally the capacity to research threats and solutions to mitigate threats. State government representatives should include law enforcement, fire services, emergency management, public health, risk management, transportation, and public services. A broad coalition of team members will insure a breadth of experience and professionalism and will act to spread the burden of inventorying and assessing infrastructure assets within the state across all interested entities. Considering the DoD's task to secure the DIB and a state's obligation to assist the DoD in that regard, the state's National Guard should have representatives on the teams.

The National Guard represents a broad spectrum of skill sets relevant to CIP, such as structural engineers, water and waste water treatment specialists, chemical munitions experts, intelligence analysts, law enforcement specialists, special operations forces with an appreciation of enemy nations and terrorist courses of action. More importantly, the military has a strong tradition of organizing complex tasks, developing strategies to affect goals, prioritizing effort, and leading complex programs. The military skill sets would enhance the IA program and provide an additional cross-learning opportunity for state CIP practitioners.

The stable of IA program members could be likened to members of an orchestra with honed skills that—without organization—will not produce a symphony. Much like an orchestra is led by a maestro, the IA program will require a leader to arrange the appropriate scores or plans, cultivate members' skills, and blend the skills to achieve an effective program. Massachusetts will need to find a homeland security maestro to lead the IA program.

D. STATE INFRASTRUCTURE PROGRAM LEADER

In Massachusetts, the current CIP program is directed by the state police, out of the Commonwealth Fusion Center. The state CIP program should become the infrastructure assurance program within the Secretary of Public Safety's office, directed by the Under Secretary for Homeland Security. The under secretary is better positioned to engender the cooperation and goodwill of the many entities with a vested interest in CIP. The under secretary has access to the Secretary of Public Safety and by extension to the governor in the event that IA policy must be created or changed or that an errant public official needs to be guided back to the fold.

Where resilience and emergency response are important elements of assuring infrastructure services, in Massachusetts the director of the Massachusetts Emergency Management Agency could lead the state infrastructure assurance program. The leader of the program should possess the organizational skills of a maestro and should demonstrate the ability to orchestrate a multiagency, multidiscipline effort to include state agencies, the private sector, academia, and federal support. The infrastructure assurance program director would need to establish state sector-specific agencies for each of the sectors, as was done in Virginia. Like Virginia, the sector-specific agencies should be tasked to develop sector-specific plans to help guide the state effort and to organize infrastructure partnerships and work groups. The emergency management component of the infrastructure assurance program should ensure outreach to the public by exploiting each city and town's emergency manager's relationship with the local community.

An infrastructure assurance strategy requires a long-term commitment of political will and resources. A credible program and strategy is needed to maintain the support from all partners in order to be effective. Accurate threat analysis and risk management recommendations are critical to getting buy-in from the private sector and maintaining its support. The IA program manager would need to insure that his program's recommendations to infrastructure owners and operators are solidly based on facts.

To clarify, with respect to security after the 9/11 attack, the knee-jerk reaction to create physical security layers around infrastructure assets was unnecessary for many

assets and potentially a waste of money. Government-imposed physical security standards were more a demonstration of a desire to do something than a well-designed effort to implement a security program based upon an understanding of the threat and risk. However, one area that warrants the increased security attention is the cyber realm.

The Marsh Commission's focus on protecting infrastructure from the cyber threat was prescient then and remains so today. As recognized by the Marsh Commission, one area that does require physical security solutions, as well as security program and process solutions is cyber networks that connect infrastructure and SCADA systems that control them. For example, the daily operations of the power industry or water systems are controlled by SCADA systems. The state IA program director would need to ensure that strong network security protocols are exercised by state or local government–run infrastructure and to regulate network security standards for private-sector infrastructure. State infrastructure programs should develop and maintain working relationships with the regulatory agencies simply to retain situational awareness of a regulated sector's compliance with standards.

E. EDUCATE CIP PRACTITIONERS AND POLITICIANS

The current CIP practitioner's challenge to secure CIKR is compounded by a limited understanding of the composition of modern infrastructure, the interconnections and dependencies between assets within an infrastructure sector and across sectors, the nature and degree of threats that make CIKR vulnerable. There is also a lack of credible data that validates which protection actions are the most effective and resource efficient to ensure the delivery of service. The CIP practitioner should endeavor to educate himself on the types of infrastructure supporting his jurisdiction and to learn which elements of the infrastructure that, if damaged or lost, would truly create catastrophic results. An initial objective of the state strategy, then, is to promote a mechanism to develop the appropriate knowledge and skills in the infrastructure assurance program members and a corporate understanding of what is critical in the infrastructure sectors represented in Massachusetts. That corporate knowledge can be developed, consolidated, and shared in local colleges or in public-private partnerships.

The DHS offers infrastructure protection training in its CIKR Asset Protection Technical Assistance Program (CAPTAP) for infrastructure protection practitioners.[149] However, the course provides very basic knowledge and should not be seen as fulfilling the full body of requisite training for a professional infrastructure assurance team member. Additional CIKR vulnerability assessment skills can be gained through a working relationship with the National Guard and the Defense Threat Reduction Agency. IA team members could also join internationally recognized security groups like the American Society for Industrial Security (ASIS) to enhance their understanding of critical infrastructure protection, industrial security, and physical security. Undergraduate or graduate-level education in homeland security is strongly recommended. Programs such as the graduate program or the executive leadership program offered at the Center for Homeland Security at the Naval Postgraduate School in Monterey, California, should be a requisite for IA program managers. IA members' participation in online college courses in infrastructure protection should be encouraged and funded. A recommended reading list of infrastructure protection writings from professional journals, academic research, and books should be made available to further expand IA members' knowledge.

The education and research efforts undertaken by George Mason University, partnering with government and private industry, addressed earlier in this thesis, should be a model for Massachusetts to mirror in partnership with one of its local universities. State infrastructure assurance practitioners can hone their skills in such an academic relationship. In an effort like that of GMU, academics benefit from interaction with private-sector and public-sector CIP practitioners who may share ideas about the direction that research should take or whether current research is on target. Current CIP practitioners and academics can each learn from the other. Ultimately, the participation of public- and private-sector CIP practitioners in CIP educational opportunities offered at universities and colleges will foster the development of future "maestros" and "virtuosos" of homeland security.

[149] Department of Homeland Security, "CIKR Asset Protection."

The director of the state IA program should engage local and state politicians to encourage their support for the goal of statewide infrastructure assurance. Political support can be made more effective by educating politicians about infrastructure assurance. For example, an infrastructure assurance–educated politician may choose not to pursue federal funding to secure infrastructure that is not critical or that does not warrant the investment of resources solely to placate his constituents. Politicians need to discipline themselves from complicating the state CIP practitioner's efforts by attempting to unduly influence the definition of infrastructure as critical as a mechanism to acquire more federal funding. Political support and understanding of the infrastructure assurance goal may also help to eliminate the manipulation of public fears in order to gain consensus toward funding security programs that are not necessary. Politicians may best serve the infrastructure assurance effort by endorsing more research in the areas of infrastructure interdependencies, network vulnerabilities, and metrics to measure the effectiveness of infrastructure protection efforts by promoting education and training for CIP practitioners and by promoting public-private partnerships.

F. DEVELOP PUBLIC-PRIVATE PARTNERSHIPS AND SECTOR SPECIFIC COUNCILS

This thesis, the 2009 NIPP, and the infrastructure protection plans of Virginia and Washington, identify partnerships as an important component of their strategies. The state of Massachusetts should develop public-private partnerships to facilitate its infrastructure assurance initiative. The infrastructure assurance partnership should be organized along the lines of a megacommunity partnership. The megacommunity partnership concept primarily consists of three sectors: government, civil society, and business. As described by Mark Gerencser and his team, "To be effective, the megacommunity must represent and link the needs and perspectives of the three primary sectors. Order comes out of integrating and balancing the decision rights and roles of various players, that is, harnessing the dynamic tension."[150] The objective of Massachusetts state government should be to exploit the dynamic tension between the

[150] Gerencser, et al., *Megacommunities*, 57.

three primary sectors mentioned above to unify infrastructure assurance partnerships toward the goal of achieving a common interest of infrastructure assurance.

The state infrastructure assurance program should encourage the partnerships but not feel compelled to lead the partnership effort. For partnerships that include participants from academia and the private sector, principles of organization and leadership as recommended in *The Starfish and the Spider* should be considered.[151] There does not need to be a single leader for these "starfish"-like partnerships but rather a common understanding of the objective of infrastructure assurance and a corporate desire to achieve it. The partnerships should be encouraged to self-govern their actions and work cohesively toward achieving the state's strategic objectives. In these dynamic partnerships, solutions to infrastructure assurance will be discovered that are conceptually similar to discovering a "Blue Ocean"-like opportunity.[152]

Members of the partnerships should include the local DHS or other federal entities involved in a particular infrastructure sector, state government homeland security practitioners, as well as elected officials, private-sector asset owners, and academia. The following represent partnership objectives:

- Better understanding of the threat to and the vulnerabilities of infrastructure;
- Identification of which infrastructure asset's damage would result in a catastrophic event;
- Development of methods to mitigate vulnerabilities to the "critical" assets; and
- Development and fostering of a relationship based on a community of trust, where the members understand the information needs of their partners and accept that they are receiving threat information that will fulfill their objectives of ensuring the delivery of service;

[151] *The Starfish and The Spider*, by Ori Brafman and Rod A. Beckstrom, discusses the value of "starfish" organizations that succeed guided by shared interests and visions while independent of a rigid leadership hierarchy.

[152] The "Blue Ocean" concept is generally applicable to business opportunities that recognize new ideas to solve an existing problem or new market space to exploit in order to achieve success. Infrastructure assurance partnerships can create innovative ways to assure the delivery of infrastructure service. See, Kim and Mauborgne, *Blue Ocean Strategy*.

- Promotion of research to understand the jurisdiction's infrastructure and network interconnectivity issues; and
- Promotion of effective leadership in the homeland security environment.

In addition to developing partnerships, the state of Massachusetts would be well served to develop state sector-specific councils (SSSC) as did Virginia and Washington. The directors of the SSSCs would report to the director of the state infrastructure assurance program. One significant benefit of the SSSC is that the state is able to delegate responsibility for providing oversight of an entire infrastructure sector to an SSSC working on behalf of the state infrastructure assurance program. The director of the SSSC would function similarly to the section leader of an orchestra. He would be expected to prepare his associated infrastructure sector to perform at the direction of the state infrastructure protection maestro. The infrastructure assurance effort is too complex for one individual to manage without SSSCs.

G. INFORMATION SHARING TO CREATE TRUST

Information sharing issues in the homeland security environment are generally oriented around concerns about the federal government sharing intelligence and threat information with state government, with the private sector, or across any combination of those partners**.** The intelligence sharing concern is real in the minds of many homeland security partners. Accurate intelligence at the strategic, operational, and tactical level is necessary for infrastructure protection practitioners to develop appropriate security programs to mitigate potential threats. The intelligence needs to be accurate to help the infrastructure assurance effort focus protection resources where they are needed to deter or mitigate a real threat. The fact that many private-sector asset owners do not get actionable intelligence leads them to conclude that the government is unwilling to share relevant intelligence with them, rather than understanding that they are not getting the intelligence they expect because that type of intelligence is not available.

Although not specifically proposed for intelligence sharing, the concept of "trusted information sharing platforms," as proposed by Branscomb and Michel-Kerjan and addressed in Chapter IV of this thesis, could be a mechanism for ensuring that all the

partners in the state's infrastructure assurance effort are comfortable that they have the best available intelligence of the likely threats at their facilities. The intelligence should also identify whether there is a known threat against specific facilities or types of facilities. State government needs to develop trusting relationships where its private-sector partners accept that, when the state has actionable intelligence of a direct and predictable threat to their industry, they will be apprised of the information.

In addition to intelligence information, more generalized information sharing is a necessary practice to achieve infrastructure protection and the assured delivery of service. For example, a public-private infrastructure assurance partnership should regularly share ideas on how to most effectively work together. According to a recent research report by the Multi-modal Information Sharing Team for the Boston area, "Participants consistently want information that will help them improve their operational decision making."[153] The Virginia Infrastructure Protection Plan recognizes the value of information sharing and recommends that partnerships be used to "exchange ideas, approaches, and best practices."[154]

Toward that end there has been extensive research undertaken to develop effective intelligence and threat information sharing processes. Important research by the Multimodal Information Sharing Team (MIST) at the Naval Postgraduate School is being conducted on behalf of the DHS to understand the information sharing needs of homeland security partners. A recently released MIST report articulates the results of their ongoing research enhanced by research conducted during a Boston-based work group. Collaborative capacity is identified as a necessity for effective information sharing. The recent report stresses that, to develop collaborative capacity, leadership involvement is necessary in the five domains of strategy and purpose, structure, lateral mechanisms, reward systems, and people. Leadership in this effort is clearly a role for the state of Massachusetts to undertake.

---

[153] Salem, et al., *Multimodal Information Sharing Team*, 5.

[154] Commonwealth of Virginia, *Critical Infrastructure Protection*, 5.

Additional recommendations from the Boston MIST report should be factored into the Massachusetts infrastructure assurance strategy and program. For example, the workshop identified that participants believed that a formalized reward system recognizing collaborative efforts would encourage long-term participation from participants. The state infrastructure assurance program should insure that public-private collaboration receives appropriate rewards, whether through monetary recognition or through tax breaks. Ultimately, effective information sharing will have a strategic effect on the state's overall infrastructure assurance goal and should remain a priority effort throughout.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Auerswald, Philip E., Lewis M. Branscomb, Todd M. LaPorte, and Erwann O. Michel-Kerjan. "The Challenge of Protecting Critical Infrastructure." *Issues in Science and Technology Online*. Retrieved October 12, 2011, from http://www.issues.org/22.1/auerswald.html.

———. The Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability. Cambridge: Cambridge University Press, 2006.

———. "Where Private Efficiency Meets Public Vulnerability." In *The Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, edited by Phillip E. Auerswald, et al. Cambridge: Cambridge University Press, 2006.

Baldwin, Craig, Larry Irons, and Philip J. Palin. *Catastrophe, Preparation and Prevention for Law Enforcement Professionals*. Boston: McGraw-Hill, 2008.

Barrett, Paul M., and Justin Blum. "The Oil Spill: Will BP Face Criminal Charges?" *Business Week,* July 7, 2010. Retrieved July 10, 2011, from www.businessweek.com/magazine/content/10_28/b4186024400208.htm.

Bellavita, Christopher. "How Proverbs Damage Homeland Security." *Homeland Security Affairs* 7:1–10, *The 9/11 Essays*, 2011. Retrieved September 20, 2011 from http://www.hsaj.org/?article=7.2.3.

Brafman, Ori, and Rod A. Beckstrom. *The Starfish and the Spider*. New York: Penguin, 2006.

Branscomb, Lewis M., and Erwann O. Michel-Kerjan. "Public-Private Collaboration on a National and International Scale." In *The Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, ed. Phillip E. Auerswald, et al. Cambridge: Cambridge University Press, 2006.

Brown, Kathi Ann. Critical Path: A Brief History of Critical Infrastructure Protection in the United States. Arlington, VA: George Mason University Press, 2006.

Bryson, John M. Strategic Planning for Public and Nonprofit Organizations. San Francisco: Jossey-Bass, 2004.

"Commonwealth of Massachusetts State Homeland Security Strategy." 2007. Retrieved July 17, 2011, from www.mass.gov/Eeops/docs/helpus_helpyou/state_homeland_security_strategy092307.pdf.

Commonwealth of Virginia. *Critical Infrastructure Protection and Resiliency Strategic Plan.* Retrieved August 8, 2011, from http://www.vahs.virginia.gov/docs/VA_Plan.pdf.

"Critical Infrastructure and Key Assets: Definition and Identification," *Congressional Research Service Report for Congress*, October 1, 2004.

"Critical Infrastructure Protection, DHS Efforts to Assess and Promote Resiliency Are Evolving but Program Management Could Be Strengthened." 2010. Retrieved September 15, 2011, from www.gao.gov/new.items/d10772.pdf.

Department of Defense Directive 3020.40. Defense Critical Infrastructure Program. Washington D.C.: Department of Defense, 2005.

Department of Energy. "Energy Timeline 2003." Retrieved July 2, 2008, from http://www.doe.gov/about/timeline2003.htm.

Department of Homeland Security. "CIKR Asset Protection Technical Assistance Program." Retrieved August 17, 2011, from www.dhs.gov/files/programs/gc_1195679577314.shtm.

———. "Homeland Infrastructure Threat and Analysis Center." Retrieved August 10, 2011, from http://www.dhs.gov/xabout/structure/gc_1257526699957.shtm.

———. *National Infrastructure Protection Plan.* Washington, DC: U.S. Government Printing Office, 2006.

———. "A Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal and Territorial Level." 2008. Retrieved March 12, 2012, from http://www.dhs.gov/xlibrary/assets/nipp_srtitt_guide.pdf.

———. *National Infrastructure Protection Plan.* Washington, DC: U.S. Government Printing Office, 2009.

———. "Office of Infrastructure Protection." n.d. Retrieved July 31, 2010, from www.dhs.gov/xabout/structure/gc_1197658542121.shtm.

Deutch, John M. *Worldwide Threat Assessment Brief to Senate Select Committee on Intelligence.* February 22, 1996. Retrieved July 15, 2008, from https://www.cia.gov/news-information/speeches-testimony/1996/dci_speech_022296.html.

Executive Order 13010, Critical Infrastructure Protection. July 15, 1996. Retrieved January 18, 2008, from www.fas.org/irp/offdocs/eo13010.htm.

"The Federal Response to Hurricane Katrina: Lessons Learned." 2006. Retrieved June 2, 2010, from http://georgewbush-whitehouse.archives.gov/reports/katrina-lessons-learned/.

Flynn, Stephen E. "The Brittle Superpower." In *The Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, ed. Phillip E. Auerswald, et al. Cambridge: Cambridge University Press, 2006.

Friedman, Arthur R. "A Way to Operationalize the DoD's Critical Infrastructure Protection Program Using Information Assurance Policies and Technologies." US Army War College. 2005. Retrieved March 21, 2009, from http://www.strategicstudiesinstitute.army.mil/pdffiles/ksil70.pdf.

Frosch, Robert A. "Notes Toward a Theory of the Management of Vulnerability." In *The Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, ed. Phillip E. Auerswald, et al., Cambridge: Cambridge University Press, 2006.

Gerencser, Mark, Reginald Van Lee, Fernando Napolitano, and Christopher Kelly. *Megacommunities: How Leaders of Government, Business and Non-Profits Can Tackle Today's Global Challenges Together*. New York: Palgrave MacMillan, 2008.

Gorman, Sean P. "A Cyber Threat to National Security?" In *The Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, ed. Phillip E. Auerswald, et al. Cambridge: Cambridge University Press, 2006.

Government Accountability Office. "Defense Critical Infrastructure: DOD's Risk Analysis of Its Critical Infrastructure Omits Highly Sensitive Assets." GAO-08-373R Defense Critical Infrastructure. April 2, 2008.

Government Accounting Office. Testimony Before the House Committee on Homeland Security, Subcommittee on Economic Security, Infrastructure Protection, and Cyber Security, Critical Infrastructure Protection-DHS Leadership Needed to Enhance Cyber-security. Washington D.C.: Government Accounting Office, 2006. Retrieved September 22, 2009, from http://www.gao.gov/new.items/d061087t.pdf.

"Homeland Security." Joint Publication 3-26, August 2, 2005. Retrieved May 29, 2009, from http://www.dtic.mil/doctrine/jel/new_pubs/jp3_26.pdf.

Homeland Security Council. "The National Strategy for Homeland Security." October 2007. Retrieved July 17, 2009, from www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf.

Hopkins, Barry. *State Official's Guide to Critical Infrastructure Protection.* Lexington, KY: Council of State Governments.

Jaksec, Gregory M. "Public-Private-Partnering in Critical Infrastructure Protection." Master's thesis, Naval Postgraduate School, 2006.

"Keller at Large: How to Fix Routine Power Outage Issues," *CBS Boston*, October 31, 2011. Retrieved November 3, 2011, from http://boston.cbslocal.com/2011/10/31/keller-large-how-to-fix-routine-power-outage-issues/.

Kennett, Milagros Nanita, et al.. *Risk Assessment*. Risk Management Series, FEMA 452, Federal Emergency Management Agency, 2005.

Kim, W. Chan, and Mauborgne, Renee. Blue Ocean Strategy: How to Create Uncontested Market Space and Make the Competition Irrelevant. Boston: Harvard Business School Press, 2005.

La Porte, Todd M. "Challenges of Assuring High Reliability When Facing Suicidal Terrorism." In *The Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, ed. Phillip E. Auerswald, et al., Cambridge: Cambridge University Press, 2006.

———. "Managing for the Unexpected." In *The Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, ed. Phillip E. Auerswald, et al. Cambridge: Cambridge University Press, 2006.

Lewis, Ted G. *Critical Infrastructure Protection in Homeland Security*. Hoboken, NJ: John Wiley and Sons, 2006.

Lopez, Brian. "Critical Infrastructure Protection in the United States Since 1993." In *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, ed. Philip E. Auerswald, et al., Cambridge: Cambridge University Press, 2006.

MacDonald, James W. "Terrorism, Insurance, and Preparedness—Connecting the Dots." In *The Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, ed. Phillip E. Auerswald, et al., Cambridge: Cambridge University Press, 2006.

Markoff, John, David E. Sanger, and Thom Shanker. "In Digital Combat, U.S. Finds No Easy Deterrent." *New York Times*, January 25, 2010. Retrieved Aril 23, 2010, from www.nytimes.com/2010/01/26/world/26cyber.html?pagewanted=1&_r=1&ref=todayspaper.

Marsh, Robert. "Foreword." In *The Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, edited by Phillip E. Auerswald, et al. Cambridge: Cambridge University Press, 2006.

Masse, Todd, Siobhan O'Neil, and John Rollins. "The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues and Options for Congress." *Congressional Research Service Report for Congress*. Washington D.C.: Library of Congress, 2007.

McNeil, Jena Baker, and Richard Weitz. "How to Fix Critical Infrastructure Protection Plans: A Guide for Congress." *Backgrounder*, Heritage Foundation No. 2404, 2010.

Michel-Kerjan, Erwann O. "Insurance, The 14th Critical Sector." In *The Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, ed. Phillip E. Auerswald, et al. Cambridge: Cambridge University Press, 2006.

Minkel, J. R. "The 2003 Northeast Blackout—Five Years Later." *Scientific American*, August 13, 2008. Retrieved August 30, 2009, from www.scientificamerican.com/article.cfm?id=2003-blackout-five-years-later.

National Academies Press. "Review of the Department of Homeland Security's Approach to Risk Analysis." 2010. Retrieved September 20, 2011, from www.nap.edu/openbook.php?record_id=12972.

"The National Guard's Role in Homeland Defense." n.d. Retrieved August 16, 2010, from www.ng.mil/features/HomelandDefense/cip-maa/factsheet.html.

"National Response Framework." 2008. Retrieved July 20, 2010, from www.fema.gov/pdf/emergency/nrf/nrf.core.pdf.

"National Security Strategy." 2010. Retrieved August 26, 2011, from www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf .

"Office of the Under Secretary of Defense for Policy." Retrieved March 2, 2012, from http://policy.defense.gov/hdasa/dcip/partnering.aspx.

"Operation Desert Storm: Evaluation of Air Campaign." Letter Report, 06/12/97, GAO/NSIAD-97-134. Retrieved January 10, 2010, from www.fas.org/man/gao/nsiad97134/app_05.htm.

Pfeiffer, Sacha, and Lynn Jolicoeur. "Why Local Power Utilities Often Outperform Regional Ones." *Boston NPR*. Retrieved November 10, 2011, from http://www.wbur.org/2011/11/04/municipal-power.

"Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence." Department of Defense Directive 0-2000.12-H, February 1993.

"Report to the President and Congress on the Protection of US Forces Abroad, Annex A-The Downing Investigation Report." 1996. Retrieved February 8, 2008, from www.fas.org/irp/threat/downing/report.pdf.

Salem, Anita, Susan Hocevar, Wendy Walsh, Lyla Englehorn, and Sarah Martin. "Multimodal Information Sharing Team, Port of Boston, Industry and Public Sector Cooperation and Information Sharing." 2011. Retrieved November 29, 2011, from http://www.linkedin.com/news?viewArticle=&articleID=709191309&gid=3771704&type=member&item=66622348&articleURL=https%3A%2F%2Fwww%2Ebox%2Enet%2Fshared%2Fbuoyl6svxed8czuh2sr3&urlhash=Sm_o&trk=group_most_popular-0-b-shrttl.

State of Arizona, "2006 Interim State Infrastructure Protection Plan." 2006. Retrieved June 12, 2009, from http://www.homelandsecurity.az.gov/documents/ReportsDocs/120606_SIPPActive.pdf.

Stockton, Paul. "Ten Years After 9/11: Challenges for the Decade to Come." *Homeland Security Affairs* 7, The 9/11 Essays. September 2011. Retrieved October 20, 2011, from www.hsaj.org/?article=7.2.11.

Sun-Tzu. *Art of War*, trans. by Ralph D. Sawyer. San Francisco: Westview Press, 1994.

USA Patriot Act (H.R. 3162). Retrieved January 28, 2008, from http://epic.org/privacy/terrorism/hr3162.html.

"Washington Infrastructure Protection Plan." 2008. Retrieved August 10, 2011, from http://www.emd.wa.gov/plans/documents/WAHLSStrategic2006-2011.pdf.

"Washington Statewide Homeland Security Strategy." 2006–2011. Retrieved August 10, 2011, from http://www.emd.wa.gov/grants/documents/2006-2011-team-wa-hls-strategic-plan.pdf.

The White House. *Homeland Security Presidential Directive-7, Critical Infrastructure Identification, Prioritization, and Protection.* Washington D.C.: 2003. Retrieved July 17, 2009, from www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1.

———. The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets. Washington, DC: U.S. Government Printing Office, 2003.

———. *Protecting America's Critical Infrastructure, Presidential Decision Directive/NSC-63*, Washington D.C.: Critical Infrastructure Assurance Office, 1998. Retrieved January 21, 2008, from www.fas.org/irp/offdocs/pdd/pdd-63.htm.

White House Office of Homeland Security. *The National Strategy for Homeland Security*. 2002. Retrieved March 14, 2009, from www.dhs.gov/xlibrary/assets/nat_strat_hls.pdf.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Kurt Schwartz, Undersecretary for Public Safety
   Executive Office of Public Safety and Security
   State of Massachusetts
   Boston, Massachusetts

4. Christopher Bellavita
   Center for Homeland Defense and Security
   Naval Postgraduate School
   Monterey, California

5. Ted Lewis
   Center for Homeland Defense and Security
   Naval Postgraduate School
   Monterey, California